Euroopan unionin
neuvosto

Bryssel, 18. heinäkuuta 2022
(OR. en)

11468/22
ADD 1

AVIATION 171
DELACT 120

SAATE

Lähettäjä:	Euroopan komission pääsihteeri, allekirjoittajana johtaja Martine DEPREZ
Saapunut:	14. heinäkuuta 2022
Vastaanottaja:	Neuvoston pääsihteeristö
Kom:n asiak. nro:	C(2022) 4882 final – LIITE
Asia:	LIITE asiakirjaan KOMISSION DELEGOITU ASETUS 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

Valtuuskunnille toimitetaan oheisena asiakirja C(2022) 4882 final – LIITE.

Liite: C(2022) 4882 final – LIITE

EUROOPAN
KOMISSIO

Bryssel 14.7.2022
C(2022) 4882 final

ANNEX

LIITE

asiakirjaan

KOMISSION DELEGOITU ASETUS

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

LIITE

TIETOTURVA – ORGANISAATIOTA KOSKEVAT VAATIMUKSET

[OSA IS.D.OR]

IS.D.OR.100 Soveltamisala

Tässä osassa vahvistetaan vaatimukset, jotka tämän asetuksen 2 artiklassa tarkoitettujen organisaatioiden on täytettävä.

IS.D.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.D.OR.205 kohdan mukaisesti;

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

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

5) määrittelee ja ottaa käyttöön tarvittavat toimenpiteet tietoturvatapahtumien havaitsemiseksi IS.D.OR.220 kohdan mukaisesti ja tunnistaa ne tapahtumat, joita pidetään sellaisina vaaratilanteina, joilla saattaa olla vaikutusta ilmailun turvallisuuteen, lukuun ottamatta IS.D.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.D.OR.225 kohdan mukaisesti;

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

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

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

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

12) valvoo, että organisaatio täyttää tämän asetuksen vaatimukset, ja antaa havainnoista palautetta vastuulliselle johtajalle tai suunnitteluorganisaatioiden osalta suunnitteluorganisaation päällikölle korjaavien toimien tehokkaan toteuttamisen 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.D.OR.260 kohdan mukainen jatkuvan parantamisen prosessi.

c) Organisaation on IS.D.OR.250 kohdan mukaisesti dokumentoitava kaikki IS.D.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.D.OR.255 kohdan mukaisesti.

d) Niiden prosessien, menettelyjen, tehtävien ja vastuiden, jotka organisaatio on laatinut IS.D.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 asiaan liittyviä vaatimuksia IS.D.OR.205–IS.D.OR.260 kohdassa, 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[1] sisältyvät ilmoitusvaatimukset ja IS.D.OR.200 kohdan a alakohdan 13 alakohdan vaatimukset. Hyväksynnän on perustuttava organisaation tai kolmannen osapuolen IS.D.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.D.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.

[1] Euroopan parlamentin ja neuvoston asetus (EU) N:o 376/2014, annettu 3 päivänä huhtikuuta 2014, poikkeamien ilmoittamisesta, analysoinnista ja seurannasta siviili-ilmailun alalla, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 996/2010 muuttamisesta sekä Euroopan parlamentin ja neuvoston direktiivin 2003/42/EY, komission asetusten (EY) N:o 1321/2007 ja (EY) N:o 1330/2007 kumoamisesta (EUVL L 122, 24.4.2014, s. 18).

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.D.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 c 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.

IS.D.OR.210 Tietoturvariskien käsittely

a) Organisaation on laadittava toimenpiteet IS.D.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.D.OR.240 kohdan a ja b alakohdassa tarkoitetulle henkilölle ja muulle organisaation henkilöstölle, jota asia koskee, on annettava tieto IS.D.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.D.OR.205 kohdan b alakohdan mukainen rajapinta.

IS.D.OR.215 Tietoturvaa koskeva sisäinen ilmoitusjärjestelmä

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

b) Tämän järjestelmän ja IS.D.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.D.OR.205 ja IS.D.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.D.OR.220 Tietoturvapoikkeamat — havaitseminen, reagointi ja palautuminen

a) Organisaation on IS.D.OR.205 kohdan mukaisesti tehdyn riskinarvioinnin tulosten ja IS.D.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.D.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.D.OR.205 kohdan a alakohdassa määritellyt kohteena olevat osa-alueet turvalliseen tilaan organisaation ennalta määrittelemässä palautumisajassa.

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

a) Saatuaan toimivaltaiselta viranomaiselta ilmoituksen havainnoista organisaation on

1) tunnistettava havaitun vaatimustenvastaisuuden 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.D.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.D.OR.235 Tietoturvan hallinnan teettäminen alihankintana

a) Teetettäessä osa IS.D.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.D.OR.240 Henkilöstövaatimukset

a) Organisaation vastuullisella johtajalla tai suunnitteluorganisaatioiden osalta suunnitteluorganisaation päälliköllä, joka on tämän asetuksen 2 artiklan 1 kohdan a ja b alakohdassa tarkoitetusti nimetty asetuksen (EU) N:o 748/2012 ja asetuksen (EU) N:o 139/2014 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.D.OR.200 kohdan a alakohdan 1 alakohdassa tarkoitettu tietoturvapolitiikka ja edistettävä sitä;

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

b) Vastuullisen johtajan tai suunnitteluorganisaatioiden osalta suunnitteluorganisaation päällikön on nimitettävä henkilö tai henkilöryhmä varmistamaan, että organisaatio täyttää tämän asetuksen vaatimukset, ja määriteltävä heidän valtuuksiensa laajuus. Kyseisen henkilön tai henkilöryhmän on raportoitava suoraan vastuulliselle johtajalle tai suunnitteluorganisaatioiden osalta suunnitteluorganisaation päällikölle, 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 tai suunnitteluorganisaatioiden osalta suunnitteluorganisaation päällikön on nimitettävä henkilö tai henkilöryhmä, joka vastaa IS.D.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 tai suunnitteluorganisaatioiden osalta suunnitteluorganisaation päällikkö voi delegoida toimintansa yhteiselle vastuuhenkilölle.

Tällöin organisaation vastuullisen johtajan tai suunnitteluorganisaatioiden osalta suunnitteluorganisaation päällikön ja yhteisen vastuuhenkilön välillä on otettava käyttöön koordinointitoimenpiteet tietoturvan hallinnan asianmukaisen integroinnin varmistamiseksi organisaatiossa.

e) Vastuullisella johtajalla tai suunnitteluorganisaation päälliköllä taikka d alakohdassa tarkoitetulla yhteisellä vastuuhenkilöllä on oltava valtuudet luoda yrityksen puolesta IS.D.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.D.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.D.OR.200 kohdan e alakohdan mukaiset mahdollisesti saadut hyväksynnät ja niihin liittyvät tietoturvariskien arvioinnit;

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

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

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

v) tiedot IS.D.OR.215 ja IS.D.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.D.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 tai suunnitteluorganisaatioiden osalta suunnitteluorganisaation päällikön allekirjoittaman lausunnon, jossa vahvistetaan, että organisaatio työskentelee kaikkina aikoina tämän liitteen ja tietoturvan hallinnan käsikirjan mukaisesti. Jos vastuullinen johtaja tai suunnitteluorganisaatioiden osalta suunnitteluorganisaation päällikkö ei ole organisaation pääjohtaja, pääjohtajan on allekirjoitettava lausunto;

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

3) IS.D.OR.240 kohdan d alakohdassa tarkoitetun yhteisen vastuuhenkilön, jos sellainen on, tehtävänimike, nimi, työtehtävät, vastuuvelvollisuudet, vastuualueet ja valtuudet;

4) IS.D.OR.200 kohdan a alakohdan 1 alakohdassa tarkoitettu organisaation tietoturvapolitiikka;

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

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

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

8) kuvaus IS.D.OR.215 kohdassa tarkoitetusta sisäisestä ilmoitusjärjestelmästä;

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

i) IS.D.OR.200 kohdan c alakohdassa tarkoitettu dokumentointi;

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

iii) c alakohdassa määritelty tietoturvan hallinnan käsikirjan muuttamismenettely;

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.D.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.D.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 koulutusorganisaation 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.D.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.