Az Európai Unió
Tanácsa

Brüsszel, 2022. július 18.
(OR. en)

11468/22
ADD 1

AVIATION 171
DELACT 120

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Az átvétel dátuma:	2022. július 14.
Címzett:	a Tanács Főtitkársága
Biz. dok. sz.:	C(2022) 4882 final - ANNEX
Tárgy:	MELLÉKLET a következőhöz: A BIZOTTSÁG FELHATALMAZÁSON ALAPULÓ RENDELETE az (EU) 2018/1139 európai parlamenti és tanácsi rendeletnek a 748/2012/EU és a 139/2014/EU bizottsági rendelet hatálya alá tartozó szervezetekre vonatkozó, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatok kezelésével kapcsolatos követelmények tekintetében történő alkalmazására irányadó szabályok megállapításáról, valamint a 748/2012/EU és a 139/2014/EU bizottsági rendelet módosításáról

Mellékelten továbbítjuk a delegációknak a C(2022) 4882 final számú dokumentum MELLÉKLETÉT.

Melléklet: C(2022) 4882 final - ANNEX

EURÓPAI
BIZOTTSÁG

Brüsszel, 2022.7.14.
C(2022) 4882 final

ANNEX

MELLÉKLET

a következőhöz:

A BIZOTTSÁG FELHATALMAZÁSON ALAPULÓ RENDELETE

az (EU) 2018/1139 európai parlamenti és tanácsi rendeletnek a 748/2012/EU és a 139/2014/EU bizottsági rendelet hatálya alá tartozó szervezetekre vonatkozó, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatok kezelésével kapcsolatos követelmények tekintetében történő alkalmazására irányadó szabályok megállapításáról, valamint a 748/2012/EU és a 139/2014/EU bizottsági rendelet módosításáról

MELLÉKLET

INFORMÁCIÓBIZTONSÁG – A SZERVEZETEKRE VONATKOZÓ KÖVETELMÉNYEK

[IS.D.OR RÉSZ]

IS.D.OR.100. Hatály

Ez a rész meghatározza az e rendelet 2. cikkében említett szervezetek által teljesítendő követelményeket.

IS.D.OR.200. Információbiztonsági irányítási rendszer (ISMS)

a) Az 1. cikkben meghatározott célkitűzések megvalósítása érdekében a szervezet információbiztonsági irányítási rendszert (a továbbiakban: ISMS) hoz létre, alkalmaz és tart fenn, amely biztosítja, hogy a szervezet:

   1. olyan információbiztonsági szabályokat hozzon létre, amelyek meghatározzák a szervezet általános elveit az információbiztonsági kockázatok repülésbiztonságra gyakorolt lehetséges hatásaival kapcsolatban;

   2. az IS.D.OR.205. pontnak megfelelően azonosítsa és felülvizsgálja az

információbiztonsági kockázatokat;

3. az IS.D.OR.210. pontnak megfelelően információbiztonsági kockázatkezelési intézkedéseket határozzon meg és hajtson végre;

4. az IS.D.OR.215. pontnak megfelelően információbiztonsági belső jelentéstételi rendszert alkalmazzon;

5. az IS.D.OR.220. pontnak megfelelően meghatározza és végrehajtsa az információbiztonsági események észleléséhez szükséges intézkedéseket, azonosítsa közülük azokat, amelyek az IS.D.OR.205. e) pont által megengedettek kivételével potenciálisan hatással lehetnek a repülésbiztonságra, továbbá reagáljon és megoldást találjon rájuk;

6. végrehajtsa az illetékes hatóság által a repülésbiztonságra hatást gyakorló információbiztonsági incidensekre vagy sebezhetőségre adott azonnali reagálásként bejelentett intézkedéseket;

7. az IS.D.OR.225. pontnak megfelelően meghozza a megfelelő intézkedéseket az illetékes hatóság által közölt megállapítások kezelésére;

8. az IS.D.OR.230. pontnak megfelelően külső jelentéstételi rendszert alkalmazzon annak érdekében, hogy az illetékes hatóság meghozhassa a megfelelő intézkedéseket;

9. az IS.D.OR.200. pontban említett tevékenységek bármely részére vonatkozó, más szervezetekkel létrehozott szerződések megkötésekor megfeleljen az IS.D.OR.235. pontban foglalt követelményeknek;

10. megfeleljen az IS.D.OR.240. pontban meghatározott személyzeti követelményeknek;

11. megfeleljen az IS.D.OR.245. pontban meghatározott nyilvántartási követelményeknek;

12. ellenőrizze, hogy a szervezet megfelel-e e rendelet követelményeinek, és a korrekciós intézkedések hatékony végrehajtásának biztosítása érdekében visszajelzést adjon a megállapításokról a felelős vezetőnek, illetve tervező szervezetek esetében a tervező szervezet vezetőjének;

13. a biztonsági események jelentésére vonatkozó alkalmazandó követelmények sérelme nélkül védje a szervezet más szervezetektől kapott információinak bizalmas jellegét, az adott információk érzékenységi szintjének megfelelően.

b) Az 1. cikkben említett követelmények folyamatos teljesítése érdekében a szervezet az IS.D.OR.260. pontnak megfelelően folyamatos fejlesztést végez.

c) A szervezet az IS.D.OR.250. pontnak megfelelően dokumentálja az IS.D.OR.200. a) pontnak való megfeleléshez szükséges valamennyi kulcsfontosságú folyamatot, eljárást, szerepet és felelősségi kört, és kialakítja a dokumentáció módosításának folyamatát. Az

említett folyamatokat, eljárásokat, szerepeket és felelősségi köröket érintő változásokat az IS.D.OR.255. pontnak megfelelően kell kezelni.

d) A szervezet által az IS.D.OR.200. a) pontnak való megfelelés érdekében megállapított folyamatoknak, eljárásoknak, szerepeknek és felelősségi köröknek összhangban kell lenniük a szervezet tevékenységeinek jellegével és összetettségével az e tevékenységekkel járó információbiztonsági kockázatok értékelése alapján, és azok integrálhatók a szervezet által már bevezetett egyéb meglévő irányítási rendszerekbe.

e) A 376/2014/EU rendeletben([1]) foglalt jelentéstételi követelményeknek és az IS.D.OR.200. a) 13. pontban foglalt követelményeknek való megfelelésre vonatkozó kötelezettség sérelme nélkül az illetékes hatóság jóváhagyhatja, hogy a szervezet ne hajtsa végre az a)–d) pontban említett követelményeket, valamint az IS.D.OR.205–IS.D.OR.260. pontban említett kapcsolódó követelményeket, amennyiben a szervezet a szóban forgó hatóság számára kielégítően bizonyítja, hogy tevékenységei, létesítményei és erőforrásai, valamint az általa működtetett, nyújtott, kapott és fenntartott szolgáltatások sem az adott szervezet, sem más szervezetek tekintetében nem jelentenek a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatot. A jóváhagyásnak a szervezet vagy egy harmadik fél által az IS.D.OR.205. pontnak megfelelően elvégzett és dokumentált, valamint a releváns illetékes hatóság által felülvizsgált és jóváhagyott információbiztonsági kockázatértékelésen kell alapulnia.

A jóváhagyás folyamatos érvényességét az illetékes hatóság az alkalmazandó felügyeleti ellenőrzési ciklust követően, valamint minden olyan esetben felülvizsgálja, amikor a szervezet tevékenységi körében változtatásokat hajtanak végre.

IS.D.OR.205. Információbiztonsági kockázatértékelés

a) A szervezet azonosítja minden olyan elemét, amely ki lehet téve információbiztonsági kockázatoknak. Ez a következőket foglalja magában:

1. a szervezet tevékenységei, létesítményei és erőforrásai, valamint a szervezet által működtetett, nyújtott, kapott vagy fenntartott szolgáltatások;

2. az 1. pontban felsorolt elemek működéséhez hozzájáruló berendezések, rendszerek, adatok és információk.

b) A szervezet azonosítja a közte és más szervezetek között meglévő azon kapcsolódási pontokat, amelyek információbiztonsági kockázatoknak való kölcsönös kitettséget eredményezhetnek.

c) Az a) és b) pontban említett elemek és kapcsolódási pontok tekintetében a szervezet azonosítja a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatokat. A szervezet minden egyes azonosított kockázat tekintetében:

([1]) Az Európai Parlament és a Tanács 376/2014/EU rendelete (2014. április 3.) a polgári légi közlekedési események jelentéséről, elemzéséről és nyomon követéséről, valamint a 996/2010/EU európai parlamenti és tanácsi rendelet módosításáról és a 2003/42/EK európai parlamenti és tanácsi irányelv, valamint az 1321/2007/EK bizottsági rendelet és az 1330/2007/EK bizottsági rendelet hatályon kívül helyezéséről (HL L 122., 2014.4.24., 18. o.).

1. kockázati szintet állapít meg a szervezet által előre meghatározott osztályozásnak megfelelően;

2. az egyes kockázatokat és azok szintjét társítja az a) és b) pontnak megfelelően azonosított megfelelő elemhez vagy kapcsolódási ponthoz.

Az 1. pontban említett, előre meghatározott osztályozásnak figyelembe kell vennie a fenyegetettségi forgatókönyv megvalósulásának valószínűségét és biztonsági következményeinek súlyosságát. Ezen osztályozás alapján és figyelembe véve, hogy a műveletek tekintetében a szervezet rendelkezik-e strukturált és megismételhető kockázatkezelési eljárással, a szervezetnek képesnek kell lennie annak megállapítására, hogy a kockázat elfogadható-e, vagy az az IS.D.OR.210. pontnak megfelelően kezelendő.

A kockázatértékelések kölcsönös összehasonlíthatóságának megkönnyítése érdekében a kockázati szint 1. pont szerinti megállapítása során figyelembe kell venni a b) pontban említett szervezetekkel együttműködésben szerzett releváns információkat.

d) A szervezet az alábbi helyzetek bármelyikének fennállása esetén felülvizsgálja és aktualizálja az a), b) és c) pontnak megfelelően elvégzett kockázatértékelést:

1. változás következik be az információbiztonsági kockázatoknak kitett elemek tekintetében;

2. változás következik be a szervezet és más szervezetek közötti kapcsolódási pontok vagy a többi szervezet által közölt kockázatok tekintetében;

3. változás következik be a kockázatok azonosításához, elemzéséhez és osztályozásához használt információk vagy ismeretek tekintetében;

4. tanulságok kerültek levonásra az információbiztonsági incidensek elemzéséből.

IS.D.OR.210. Információbiztonsági kockázatkezelés

a) A szervezet intézkedéseket dolgoz ki az IS.D.OR.205. ponttal összhangban azonosított elfogadhatatlan kockázatok kezelésére, azokat időben végrehajtja, és ellenőrzi folyamatos hatékonyságukat. A szóban forgó intézkedéseknek lehetővé kell tenniük a szervezet számára, hogy:

1. ellenőrizze a fenyegetettségi forgatókönyv tényleges megvalósulásához hozzájáruló körülményeket;

2. a fenyegetettségi forgatókönyv megvalósulása esetén csökkentse a repülésbiztonsági következmények súlyosságát;

3. elkerülje a kockázatokat.

Ezek az intézkedések nem jelenthetnek potenciális új elfogadhatatlan kockázatot a repülésbiztonságra nézve.

b) Az IS.D.OR.240. a) és b) pontban említett személyt és a szervezet egyéb érintett személyzetét tájékoztatni kell az IS.D.OR.205. pont szerint elvégzett kockázatértékelés eredményéről, a megfelelő fenyegetettségi forgatókönyvekről és a végrehajtandó intézkedésekről.

A szervezet emellett tájékoztatja azokat a szervezeteket, amelyekkel az IS.D.OR.205. b) pontnak megfelelően kapcsolódási ponttal rendelkezik, a mindkét szervezetet érintő kockázatokról.

IS.D.OR.215. Információbiztonsági belső jelentéstételi rendszer

a) A szervezet belső jelentéstételi rendszert hoz létre az információbiztonsági események – köztük az IS.D.OR.230. pont szerint bejelentendő események – összegyűjtésének és értékelésének lehetővé tétele érdekében.

b) A szóban forgó rendszernek és az IS.D.OR.220. pontban említett eljárásnak lehetővé kell tennie a szervezet számára, hogy:

1. megállapítsa, hogy az a) pont szerint bejelentett események közül melyek minősülnek a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági incidenseknek vagy sebezhetőségeknek;

2. azonosítsa az 1. pontnak megfelelően megállapított információbiztonsági incidensek és sebezhetőségek okait és az azokhoz hozzájáruló tényezőket, és az IS.D.OR.205. és az IS.D.OR.220. pont szerinti információbiztonsági kockázatkezelési eljárás részeként kezelje azokat;

3. biztosítsa az 1. pontnak megfelelően azonosított információbiztonsági incidensekkel és sebezhetőségekkel kapcsolatos valamennyi ismert és releváns információ értékelését;

4. szükség esetén biztosítsa az információk belső terjesztésére szolgáló módszer alkalmazását.

c) Minden olyan, szerződés keretében megbízott szervezetnek, amely a szervezetet a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatnak teheti ki, be kell jelentenie a szervezetnek az információbiztonsági eseményeket. A szóban forgó jelentéseket az egyedi szerződéses megállapodásokban meghatározott eljárások szerint kell benyújtani és a b) ponttal összhangban kell értékelni.

d) A szervezet együttműködik a vizsgálatokban minden más olyan szervezettel, amely jelentős mértékben hozzájárul saját tevékenységeinek információbiztonságához.

e) A szervezet integrálhatja ezt a jelentéstételi rendszert más, már alkalmazott jelentéstételi rendszerekbe.

IS.D.OR.220. Információbiztonsági incidensek – észlelés, reagálás és helyreállítás

a) Az IS.D.OR.205. pont szerint elvégzett kockázatértékelés és az IS.D.OR.210. szerint elvégzett kockázatkezelés eredménye alapján a szervezet intézkedéseket tesz az olyan események és sebezhetőségek észlelésére, amelyek elfogadhatatlan kockázatok lehetséges bekövetkezését jelzik, és amelyek potenciálisan hatással lehetnek a repülésbiztonságra. A szóban forgó észlelési intézkedéseknek lehetővé kell tenniük a szervezet számára, hogy:

1. azonosítsa az előre meghatározott funkcionális teljesítmény-alapértékektől való eltéréseket;

2. bármilyen eltérés esetén figyelmeztetéseket adjon a megfelelő válaszintézkedések aktiválása érdekében.

b) A szervezet intézkedéseket tesz annak érdekében, hogy valamely esemény kapcsán reagáljon az a) pontnak megfelelően azonosított bármely olyan körülményre, amelynek teljesülése esetén információbiztonsági incidens következhet vagy következett be. A szóban forgó válaszintézkedéseknek lehetővé kell tenniük a szervezet számára, hogy:

1. előre meghatározott erőforrások és intézkedések aktiválásával kezdeményezze az a) 2. pontban említett figyelmeztetésekre való reagálást;

2. megfékezze a támadás terjedését és elkerülje a fenyegetettségi forgatókönyv teljes körű megvalósulását;

3. ellenőrizze az IS.D.OR.205. a) pontban meghatározott érintett elemek meghibásodásának típusát.

c) A szervezet végrehajtja az információbiztonsági incidensek utáni helyreállítást célzó intézkedéseket, beleértve szükség esetén a vészhelyzeti intézkedéseket is. A szóban forgó helyreállítási intézkedéseknek lehetővé kell tenniük a szervezet számára, hogy:

1. megszüntesse vagy elfogadható szintre korlátozza az eseményt okozó körülményt;

2. a szervezet által előzetesen meghatározott helyreállási időn belül biztonságos állapotba hozza az IS.D.OR.205. a) pontban meghatározott érintett elemeket.

IS.D.OR.225. Reagálás az illetékes hatóság által közölt megállapításokra

a) Az illetékes hatóság által benyújtott, a megállapításokról szóló értesítés kézhezvételét követően a szervezet:

1. meghatározza a meg nem felelés kiváltó okát vagy okait, illetve az azt előidéző tényezőket;

2. korrekciós intézkedési tervet dolgoz ki;

3. az illetékes hatóság számára kielégítő módon igazolja a meg nem felelés orvoslását.

b) Az a) pontban említett intézkedéseket az illetékes hatósággal egyeztetett határidőn belül kell végrehajtani.

IS.D.OR.230. Információbiztonsági külső jelentéstételi rendszer

a) A szervezet olyan információbiztonsági jelentéstételi rendszert működtet, amely megfelel a 376/2014/EU rendeletben, valamint az ahhoz kapcsolódó felhatalmazáson alapuló és végrehajtási jogi aktusokban meghatározott követelményeknek, amennyiben a szóban forgó rendelet alkalmazandó a szervezetre.

b) A 376/2014/EU rendeletben foglalt kötelezettségek sérelme nélkül a szervezet biztosítja, hogy az illetékes hatóság bejelentést kapjon minden olyan információbiztonsági incidensről vagy sebezhetőségről, amely jelentős kockázatot jelenthet a repülésbiztonságra. Továbbá:

1. amennyiben egy ilyen incidens vagy sebezhetőség valamely légi járművet vagy kapcsolódó rendszert vagy komponenst érinti, a szervezet azt a tervjóváhagyás jogosultjának is jelenti;

2. amennyiben egy ilyen incidens vagy sebezhetőség a szervezet által használt rendszert vagy rendszerelemet érinti, a szervezet jelenti azt a rendszer vagy rendszerelem tervezéséért felelős szervezetnek.

c) A szervezet az alábbiak szerint jelenti a b) pontban említett körülményeket:

1. amint a szervezet tudomást szerez a körülményről, értesítést nyújt be az illetékes hatóságnak és adott esetben a tervjóváhagyás jogosultjának, illetve a rendszer vagy rendszerelem tervezéséért felelős szervezetnek;

2. a lehető leghamarabb, de legfeljebb 72 órával azt követően, hogy a szervezet tudomást szerez a körülményről, jelentést nyújt be az illetékes hatóságnak és adott esetben a tervjóváhagyás jogosultjának, illetve a rendszer vagy rendszerelem tervezéséért felelős szervezetnek, kivéve, ha ezt rendkívüli körülmények megakadályozzák.

   A jelentést az illetékes hatóság által meghatározott formában kell elkészíteni, és annak tartalmaznia kell a körülményre vonatkozóan a szervezet birtokában lévő valamennyi lényeges információt;

3. nyomonkövetési jelentést nyújt be az illetékes hatóságnak és adott esetben a tervjóváhagyás jogosultjának, illetve a rendszer vagy rendszerelem tervezéséért felelős szervezetnek, amelyben részletesen ismerteti azokat az intézkedéseket, amelyeket a szervezet az incidens utáni helyreállítás érdekében tett vagy szándékozik tenni, valamint a hasonló információbiztonsági incidensek jövőbeli megelőzése érdekében tervezett intézkedéseket.

   A nyomonkövetési jelentést az intézkedések meghatározását követően azonnal be kell nyújtani, és az illetékes hatóság által meghatározott formában kell elkészíteni.

IS.D.OR.235. Információbiztonsági irányítási tevékenységek kiszervezése

a) A szervezet biztosítja, hogy az IS.D.OR.200. pontban említett tevékenységek bármely részére vonatkozó, más szervezetekkel létrehozott szerződések megkötésekor a kiszervezett tevékenységek megfeleljenek e rendelet követelményeinek, és a megbízott szervezet a megbízó szervezet felügyelete alatt működjön. A szervezet biztosítja a kiszervezett tevékenységekkel kapcsolatos kockázatok megfelelő kezelését.

b) A szervezet biztosítja, hogy az illetékes hatóság kérésre felvehesse a kapcsolatot a megbízott szervezettel az e rendeletben meghatározott alkalmazandó követelményeknek való folyamatos megfelelés ellenőrzése céljából.

IS.D.OR.240. Személyzeti követelmények

a) Az e rendelet 2. cikke (1) bekezdésének a) és b) pontjában említett szervezet felelős vezetője, illetve tervező szervezetek esetében a tervező szervezet vezetője, aki a 748/2012/EU rendelettel és az 139/2014/EU rendelettel összhangban kerül kijelölésre, vállalati felhatalmazással rendelkezik annak biztosítására, hogy az e rendeletben előírt valamennyi tevékenység finanszírozható és elvégezhető legyen. A szóban forgó személy:

1. biztosítja, hogy minden szükséges erőforrás rendelkezésre álljon az e rendelet követelményeinek való megfeleléshez;

2. kidolgozza és előmozdítja az IS.D.OR.200. a) 1. pontban említett információbiztonsági szabályokat;

3. igazolja, hogy e rendeletet illetően rendelkezik az alapvető ismeretekkel.

b) A felelős vezető, illetve tervező szervezetek esetében a tervező szervezet vezetője kijelöl egy vagy több személyt annak biztosítására, hogy a szervezet megfeleljen e rendelet követelményeinek, és meghatározza az érintett(ek) hatáskörét. E személy(ek) közvetlenül a felelős vezetőnek, illetve tervező szervezetek esetében a tervező szervezet vezetőjének számol(nak) be, és rendelkezik/rendelkeznek a feladatai(k) ellátásához szükséges megfelelő ismeretekkel, háttérrel és tapasztalattal. Az eljárásokban meg kell határozni, hogy az adott személyek hosszabb távolléte esetén ki helyettesíti őket.

c) A felelős vezető, illetve tervező szervezetek esetében a tervező szervezet vezetője kijelöl egy vagy több személyt, aki(k) az IS.D.OR.200. a) 12. pontban említett megfelelőség-ellenőrzés irányításáért felel(nek).

d) Amennyiben a szervezet információbiztonsági szervezeti struktúrákat, szabályokat, folyamatokat és eljárásokat oszt meg más szervezetekkel vagy saját szervezete olyan területeivel, amelyekre nem terjed ki a jóváhagyás vagy a nyilatkozat, a felelős vezető, illetve tervező szervezetek esetében a tervező szervezet vezetője átruházhatja tevékenységét egy közös felelős személyre.

Ebben az esetben az információbiztonság-irányítás szervezeten belüli megfelelő integrációjának biztosítása érdekében meg kell határozni a szervezet felelős vezetője, illetve tervező szervezetek esetében a tervező szervezet vezetője és a közös felelős személy közötti koordinálási intézkedéseket.

e) A felelős vezető vagy a tervező szervezet vezetője vagy a d) pontban említett közös felelős személy vállalati felhatalmazással rendelkezik az IS.D.OR.200. pont végrehajtásához szükséges szervezeti struktúrák, szabályok, folyamatok és eljárások kialakítására és fenntartására.

f) A szervezetnek rendelkeznie kell egy olyan eljárással, amely biztosítja, hogy elegendő személyzet álljon rendelkezésre az e melléklet hatálya alá tartozó tevékenységek elvégzéséhez.

g) A szervezetnek rendelkeznie kell egy olyan eljárással, amely biztosítja, hogy az f) pontban említett személyzet rendelkezzen a feladatai ellátásához szükséges szakértelemmel.

h) A szervezetnek rendelkeznie kell egy olyan eljárással, amely biztosítja, hogy a személyzet elismerje a kijelölt szerepekhez és feladatokhoz kapcsolódó felelősségi köröket.

i) A szervezet biztosítja, hogy az információs rendszerekhez és az e rendelet követelményeinek hatálya alá tartozó adatokhoz hozzáféréssel rendelkező személyzet megfelelő és megbízható legyen.

IS.D.OR.245. Nyilvántartás

a) A szervezet nyilvántartást vezet információbiztonsági irányítási tevékenységeiről.

1. A szervezet biztosítja a következő nyilvántartások archiválását és nyomon követhetőségét:

i. az IS.D.OR.200. e) ponttal összhangban kapott jóváhagyások és a kapcsolódó információbiztonsági kockázatértékelés;

ii. az IS.D.OR.200. a) 9. pontban említett tevékenységekre vonatkozó szerződések;

iii. az IS.D.OR.200. d) pontban említett kulcsfontosságú folyamatokkal kapcsolatos nyilvántartások;

iv. az IS.D.OR.205. pontban említett kockázatértékelés eredményeképpen azonosított kockázatok, valamint az IS.D.OR.210. pontban említett kapcsolódó kockázatkezelési intézkedések nyilvántartása;

v. az IS.D.OR.215. és az IS.D.OR.230. pontban említett jelentéstételi rendszerekkel összhangban bejelentett információbiztonsági incidensek és sebezhetőségek nyilvántartása;

vi. azon információbiztonsági események nyilvántartása, amelyeket újra kell értékelni a fel nem tárt információbiztonsági incidensek vagy sebezhetőségek feltárása érdekében.

2. Az 1. pont i. alpontjában említett nyilvántartásokat a jóváhagyás érvényességének

megszűnését követően legalább öt évig meg kell őrizni.

3. Az 1. pont ii. alpontjában említett nyilvántartásokat a szerződés módosítását vagy megszüntetését követően legalább öt évig meg kell őrizni.

4. Az 1. pont iii., iv. és v. alpontjában említett nyilvántartásokat legalább 5 évig meg kell őrizni.

5. Az 1. pont vi. alpontjában említett nyilvántartásokat mindaddig meg kell őrizni, amíg ezeket az információbiztonsági eseményeket a szervezet által megállapított eljárásban meghatározott rendszerességgel újraértékelik.

b) A szervezet nyilvántartást vezet az információbiztonsági irányítási tevékenységekben részt vevő saját személyzetének képesítéséről és tapasztalatáról.

1. A személyzet képesítéséről és tapasztalatáról vezetett nyilvántartást mindaddig meg kell őrizni, amíg az adott személy a szervezetnél dolgozik, és legalább három évig azt követően, hogy az adott személy elhagyta a szervezetet.

2. A személyzet tagjai számára – kérésükre – hozzáférést kell biztosítani egyéni nyilvántartásaikhoz. Ezen túlmenően, amikor az említett személyek elhagyják a szervezetet, a szervezet az érintettek kérésére köteles átadni nekik a róluk vezetett egyéni nyilvántartás másolatát.

c) A nyilvántartások formátumát a szervezet eljárásaiban kell meghatározni.

d) A nyilvántartásokat oly módon kell tárolni, hogy biztosított legyen a sérüléssel, megváltoztatással és lopással szembeni védelmük, és az információk szükség esetén biztonsági besorolási szintjüknek megfelelően azonosíthatók legyenek. A szervezet gondoskodik róla, hogy a nyilvántartásokat olyan eszközökkel tárolják, amelyek biztosítják azok integritását és hitelességét, valamint az azokhoz való engedélyezett hozzáférést.

IS.D.OR.250. Információbiztonsági irányítási kézikönyv (ISMM)

a) A szervezet az illetékes hatóság rendelkezésére bocsát egy információbiztonsági irányítási kézikönyvet (a továbbiakban: ISMM) – és adott esetben bármely hivatkozott kapcsolódó kézikönyvet és eljárást –, amely a következőket tartalmazza:

1. a felelős vezető, illetve tervező szervezetek esetében a tervező szervezet vezetője által aláírt nyilatkozat, amely megerősíti, hogy a szervezet mindenkor e melléklettel és az ISMM-mel összhangban fog működni. Ha a felelős vezető, illetve tervező szervezetek esetében a tervező szervezet vezetője nem a szervezet vezérigazgatója, akkor a vezérigazgató ellenjegyzi a nyilatkozatot;

2. az IS.D.OR.240. b) és c) pontban említett személy vagy személyek beosztása, neve, feladatai, elszámoltathatósága, felelősségi köre és hatásköre;

3. adott esetben az IS.D.OR.240. d) pontban említett közös felelős személy beosztása, neve, feladatai, elszámoltathatósága, felelősségi köre és hatásköre;

4. a szervezet IS.D.OR.200. a) 1. pontban említett információbiztonsági szabályai;

5. az IS.D.OR.240. pontban előírt személyzet létszámának és kategóriáinak, valamint a személyzeti rendelkezésre állás tervezésére szolgáló rendszernek az általános leírása;

6. az IS.D.OR.200. pont végrehajtásáért felelős kulcsfontosságú személyek, köztük az IS.D.OR.200. a) 12. pontban említett megfelelés-ellenőrzésért felelős személy vagy személyek beosztása, neve, feladatai, elszámoltathatósága, felelősségi köre és hatásköre;

7. szervezeti ábra, amely bemutatja a kapcsolódó elszámoltathatósági és felelősségi láncokat a 2. és 6. pontban említett személyek tekintetében;

8. az IS.D.OR.215. pontban említett belső jelentéstételi rendszer leírása;

9. azok az eljárások, amelyek meghatározzák, hogy a szervezet hogyan biztosítja az e résznek való megfelelést, és különösen a következők:

   i. az IS.D.OR.200. c) pont szerinti dokumentáció;

   ii. azon eljárások, amelyek meghatározzák, hogy a szervezet hogyan ellenőrzi az IS.D.OR.200. a) 9. pontban említett kiszervezett tevékenységeket;

   iii. a c) pontban meghatározott ISMM-módosítási eljárás;

10. a jelenleg jóváhagyott alternatív megfelelési módozatok részletei.

b) Az ISMM első kiadását az illetékes hatóságnak jóvá kell hagynia, és annak egy példányát meg kell őriznie. Az ISMM-et szükség szerint módosítani kell annak érdekében, hogy a szervezet ISMS-ének naprakész leírása maradjon. Az ISMM módosításainak másolatát az illetékes hatóság rendelkezésére kell bocsátani.

c) Az ISMM módosításait a szervezet által megállapított eljárás szerint kell kezelni. Az ezen eljárás hatálya alá nem tartozó módosításokat és az IS.D.OR.255. b) pontban említett változásokhoz kapcsolódó módosításokat az illetékes hatóságnak jóvá kell hagynia.

d) A szervezet integrálhatja az ISMM-et a birtokában lévő egyéb irányítási szabályzatokkal vagy kézikönyvekkel, feltéve, hogy egyértelmű kereszthivatkozás áll rendelkezésre, amely jelzi, hogy az irányítási szabályzat vagy kézikönyv mely részei felelnek meg az e mellékletben foglalt különböző követelményeknek.

IS.D.OR.255. Az információbiztonsági irányítási rendszer változásai

a) Az ISMS változásait a szervezet által kidolgozott eljárás keretében lehet kezelni és bejelenteni az illetékes hatóságnak. A szóban forgó eljárást az illetékes hatóság hagyja jóvá.

b) Az ISMS-t érintő, az a) pontban említett eljárás hatálya alá nem tartozó változások tekintetében a szervezetnek kérelmeznie kell és meg kell szereznie az illetékes hatóság jóváhagyását.

E változások tekintetében:

1. a kérelmet még a változtatás végrehajtása előtt be kell nyújtani, hogy az illetékes hatóság megállapíthassa, hogy a szervezet továbbra is megfelel-e ennek a rendeletnek, és szükség esetén módosíthassa a szervezet bizonyítványát és a hozzá csatolt jóváhagyási feltételeket;

2. a szervezet az illetékes hatóság rendelkezésére bocsát minden olyan információt, amelyet az a változás értékeléséhez kér;

3. a változtatás csak az illetékes hatóság hivatalos jóváhagyásának kézhezvételét követően hajtható végre;

4. a szervezetnek az ilyen változtatások végrehajtása során az illetékes hatóság által előírt feltételek szerint kell működnie.

IS.D.OR.260. Folyamatos fejlesztés

a) A szervezet megfelelő teljesítménymutatók alkalmazásával értékeli az ISMS hatékonyságát és érettségét. Ezt az értékelést a szervezet által előre meghatározott naptári ütemezés szerint vagy egy információbiztonsági incidenst követően kell elvégezni.

b) Amennyiben az a) pontnak megfelelően elvégzett értékelést követően hiányosságokat tárnak fel, a szervezet meghozza a szükséges javító intézkedéseket annak biztosítása érdekében, hogy az ISMS továbbra is megfeleljen az alkalmazandó követelményeknek, és elfogadható szinten tartsa az információbiztonsági kockázatokat. A szervezet továbbá újraértékeli az ISMS-nek az elfogadott intézkedések által érintett elemeit.