Vijeće
Europske unije

Bruxelles, 18. srpnja 2022.
(OR. en)

11468/22
ADD 1

AVIATION 171
DELACT 120

POPRATNA BILJEŠKA

Od:	Glavna tajnica Europske komisije, potpisala direktorica Martine DEPREZ
Datum primitka:	14. srpnja 2022.
Za:	Glavno tajništvo Vijeća
Br. dok. Kom.:	C(2022) 4882 final - ANNEX
Predmet:	PRILOG DELEGIRANOJ UREDBI KOMISIJE o utvrđivanju pravila za primjenu Uredbe (EU) 2018/1139 Europskog parlamenta i Vijeća u pogledu zahtjeva za upravljanje rizicima za informacijsku sigurnost koji bi mogli utjecati na sigurnost zračnog prometa za organizacije obuhvaćene uredbama Komisije (EU) br. 748/2012 i br. 139/2014 i o izmjeni uredbi Komisije (EU) br. 748/2012 i br. 139/2014

Za delegacije se u prilogu nalazi dokument C(2022) 4882 final - ANNEX.

Priloženo: C(2022) 4882 final - ANNEX

EUROPSKA
KOMISIJA

Bruxelles, 14.7.2022.
C(2022) 4882 final

ANNEX

PRILOG

DELEGIRANOJ UREDBI KOMISIJE

o utvrđivanju pravila za primjenu Uredbe (EU) 2018/1139 Europskog parlamenta i Vijeća u pogledu zahtjeva za upravljanje rizicima za informacijsku sigurnost koji bi mogli utjecati na sigurnost zračnog prometa za organizacije obuhvaćene uredbama Komisije (EU) br. 748/2012 i br. 139/2014 i o izmjeni uredbi Komisije (EU) br. 748/2012 i br. 139/2014

PRILOG

INFORMACIJSKA SIGURNOST — ZAHTJEVI U VEZI S ORGANIZACIJAMA

[PART-IS.D.OR]

IS.D.OR.100 Područje primjene

U ovom se dijelu utvrđuju zahtjevi koje moraju ispuniti organizacije iz članka 2. ove Uredbe.

IS.D.OR.200 Sustav upravljanja informacijskom sigurnošću (ISMS)

(a) Kako bi se ostvarili ciljevi utvrđeni u članku 1. organizacija uspostavlja, primjenjuje i održava sustav upravljanja informacijskom sigurnošću (ISMS) kojim se osigurava da organizacija:

1. uspostavlja politiku informacijske sigurnosti kojom se utvrđuju opća načela organizacije u pogledu mogućeg utjecaja rizika za informacijsku sigurnost na sigurnost zračnog prometa;

2. identificira i preispituje rizike za informacijsku sigurnost u skladu s točkom IS.D.OR.205;

3. definira i provodi mjere postupanja s rizicima za informacijsku sigurnost u skladu s točkom IS.D.OR.210;

4. primjenjuje sustav unutarnjeg izvješćivanja o informacijskoj sigurnosti u skladu s točkom IS.D.OR.215;

5. u skladu s točkom IS.D.OR.220 definira i provodi mjere potrebne za otkrivanje događaja povezanih s informacijskom sigurnošću, identificira događaje koji se smatraju incidentima koji mogu utjecati na sigurnost zračnog prometa, osim u slučajevima koji su dopušteni točkom IS.D.OR.205 podtočkom (e), odgovara na te incidente i oporavlja se od njih;

6. provodi mjere koje je nadležno tijelo prijavilo kao neposrednu reakciju na incident ili ranjivost povezanu s informacijskom sigurnošću koja utječe na sigurnost zračnog prometa;

7. poduzima odgovarajuće mjere u skladu s točkom IS.D.OR.225 kako bi postupilo u skladu s nalazima koje je prijavilo nadležno tijelo;

8. primjenjuje sustav vanjskog izvješćivanja u skladu s točkom IS.D.OR.230 kako bi se nadležnom tijelu omogućilo poduzimanje odgovarajućih mjera;

9. ispunjava zahtjeve iz točke IS.D.OR.235 pri dodjeli ugovora za bilo koji dio aktivnosti iz točke IS.D.OR.200 drugim organizacijama;

10. ispunjava zahtjeve u pogledu osoblja utvrđene u točki IS.D.OR.240;

11. ispunjava zahtjeve u pogledu osoblja utvrđene u točki IS.D.OR.245;

12. prati usklađenost organizacije sa zahtjevima ove Uredbe i pruža povratne informacije o nalazima odgovornom rukovoditelju ili, u slučaju projektnih organizacija, rukovoditelju projektne organizacije kako bi se osigurala djelotvorna provedba korektivnih mjera;

13. ne dovodeći u pitanje primjenjive zahtjeve za izvješćivanje, štiti povjerljivost svih informacija koje je organizacija primila od drugih organizacija, u skladu s njihovom razinom osjetljivosti.

(b) Kako bi kontinuirano ispunjavala zahtjeve iz članka 1., organizacija provodi postupak kontinuiranog poboljšanja u skladu s točkom IS.D.OR.260.

(c) Organizacija u skladu s točkom IS.D.OR.250 dokumentira sve ključne procese, postupke, uloge i odgovornosti potrebne za usklađivanje s točkom IS.D.OR.200 podtočkom (a) i uspostavlja postupak za izmjenu te dokumentacije. Promjenama tih procesa, postupaka, uloga i odgovornosti upravlja se u skladu s točkom IS.D.OR.255.

(d) Procesi, postupci, uloge i odgovornosti koje je organizacija uspostavila radi usklađenosti s točkom IS.D.OR.200 podtočkom (a) odgovaraju prirodi i složenosti njezinih aktivnosti, na temelju procjene rizika za informacijsku sigurnost svojstvenih tim aktivnostima, i mogu se integrirati u druge postojeće sustave upravljanja koje

organizacija već primjenjuje.

(e) Ne dovodeći u pitanje obvezu ispunjavanja zahtjeva za izvješćivanje iz Uredbe (EU) br. 376/2014 ([1]) i zahtjeve iz točke IS.D.OR.200 podtočke (a) podpodtočke 13., nadležno tijelo može organizaciji izdati odobrenje za neprimjenjivanje zahtjeva iz točaka od (a) do (d) i povezanih zahtjeva iz točaka od IS.D.OR.205 do IS.D.OR.260 ako na zadovoljavajući način dokaže tom tijelu da njezine aktivnosti, objekti i resursi, kao i usluge koje pruža, prima i održava, njoj samoj ni drugim organizacijama ne predstavljaju nikakve rizike za informacijsku sigurnost koji bi mogli utjecati na sigurnost zračnog prometa. Odobrenje se temelji na dokumentiranoj procjeni rizika za informacijsku sigurnost koju je provela organizacija ili treća strana u skladu s točkom IS.D.OR.205 i pregledalo i odobrilo nadležno tijelo.

Nadležno tijelo preispitat će kontinuiranu valjanost tog odobrenja nakon primjenjivog ciklusa nadzora sigurnosti i kad god se provedu promjene u opsegu rada organizacije.

IS.D.OR.205 Procjena rizika za informacijsku sigurnost

(a) Organizacija je dužna identificirati sve svoje elemente koji bi mogli biti izloženi rizicima za informacijsku sigurnost. To uključuje:

1. aktivnosti, objekte i resurse organizacije, kao i usluge koje organizacija pruža, prima ili održava;

2. opremu, sustave, podatke i informacije koji pridonose funkcioniranju elemenata navedenih u podpodtočki 1.

(b) Organizacija mora identificirati sučelja koja ima s drugim organizacijama i koja bi mogla dovesti do međusobne izloženosti rizicima za informacijsku sigurnost.

(c) U pogledu elemenata i sučelja iz podtočaka (a) i (b), organizacija mora identificirati rizike za informacijsku sigurnost koji bi mogli utjecati na sigurnost zračnog prometa. Za svaki identificirani rizik organizacija je dužna:

1. odrediti razinu rizika u skladu s unaprijed definiranom klasifikacijom koju je utvrdila organizacija;

2. povezati svaki rizik i njegovu razinu s odgovarajućim elementom ili sučeljem utvrđenim u skladu s podtočkama (a) i (b).

U unaprijed definiranoj klasifikaciji iz podpodtočke 1. uzima se u obzir mogućnost pojave scenarija opasnosti i ozbiljnost njegovih posljedica za sigurnost. Na temelju te klasifikacije i uzimajući u obzir ima li organizacija strukturiran i ponovljiv postupak

([1]) Uredba (EU) br. 376/2014 Europskog parlamenta i Vijeća od 3. travnja 2014. o izvješćivanju, analizi i naknadnom postupanju u vezi s događajima u civilnom zrakoplovstvu, o izmjeni Uredbe (EU) br. 996/2010 Europskog parlamenta i Vijeća i stavljaju izvan snage Direktive 2003/42/EZ Europskog parlamenta i Vijeća i uredbi Komisije (EZ) br. 1321/2007 i (EZ) br. 1330/2007 (SL L 122, 24.4.2014., str. 18.).

upravljanja rizicima za operacije, organizacija može utvrditi je li rizik prihvatljiv ili je s njim potrebno postupati u skladu s točkom IS.D.OR.210.

Kako bi se olakšala međusobna usporedivost procjena rizika, pri određivanju razine rizika u skladu s podpodtočkom 1. uzimaju se u obzir relevantne informacije prikupljene u koordinaciji s organizacijama iz podtočke (b).

(d) Organizacija pregledava i ažurira procjenu rizika provedenu u skladu s podtočkama (a), (b) i (c) u bilo kojoj od sljedećih situacija:

1. došlo je do promjene elemenata koji su izloženi rizicima za informacijsku sigurnost;

2. došlo je do promjene u sučeljima između organizacije i drugih organizacija ili u rizicima koje su priopćile druge organizacije;

3. došlo je do promjene informacija ili znanja koji se upotrebljavaju za identifikaciju, analizu i klasifikaciju rizika;

4. izvučene su pouke na temelju analize incidenata povezanih s informacijskom sigurnošću.

IS.D.OR.210 Postupanje s rizicima za informacijsku sigurnost

(a) Organizacija osmišljava mjere za otklanjanje neprihvatljivih rizika identificiranih u skladu s točkom IS.D.OR.205, pravodobno ih provodi i provjerava njihovu kontinuiranu djelotvornost. Te mjere omogućuju da organizacija:

1. kontrolira okolnosti koje pridonose stvarnoj pojavi scenarija prijetnje;

2. ublaži posljedice za sigurnost zračnog prometa povezane s nastankom scenarija prijetnje;

3. izbjegava rizike.

Te mjere ne smiju uvesti nove neprihvatljive rizike za sigurnost zračnog prometa.

(b) Osoba iz točke IS.D.OR.240 podtočaka (a) i (b) i drugo uključeno osoblje organizacije obavješćuju se o ishodu procjene rizika provedene u skladu s točkom IS.D.OR.205, odgovarajućim scenarijima prijetnji i mjerama koje treba provesti.

Organizacija obavješćuje i organizacije s kojima ima sučelje u skladu s točkom IS.D.OR.205 podtočkom (b) o svim rizicima koji su zajednički objema organizacijama.

IS.D.OR.215 Sustav unutarnjeg izvješćivanja o informacijskoj sigurnosti

(a) Organizacija uspostavlja sustav unutarnjeg izvješćivanja radi prikupljanja i procjene

događaja povezanih s informacijskom sigurnošću, uključujući one o kojima treba izvješćivati u skladu s točkom IS.D.OR.230.

(b) Taj sustav i postupak iz točke IS.D.OR.220 omogućuju da organizacija:

1. identificira događaje prijavljene u skladu s podtočkom (a) koji se smatraju incidentima ili ranjivostima povezanima s informacijskom sigurnošću koji mogu utjecati na sigurnost zračnog prometa;

2. identificira uzroke incidenata i ranjivosti povezanih s informacijskom sigurnošću utvrđenih u skladu s točkom 1. i čimbenike koji im doprinose i rješava ih u okviru procesa upravljanja rizicima za informacijsku sigurnost u skladu s točkama IS.D.OR.205 i IS.D.OR.220;

3. osigura procjenu svih poznatih i relevantnih informacija koje se odnose na incidente i ranjivosti povezane s informacijskom sigurnošću i identificirane u skladu s točkom 1.;

4. osigura primjenu metode za internu distribuciju informacija prema potrebi.

(c) Svaka ugovorna organizacija koja organizaciju može izložiti rizicima za informacijsku sigurnost koji bi mogli utjecati na sigurnost zračnog prometa mora organizaciju izvijestiti o događajima povezanima s informacijskom sigurnošću. Ta se izvješća podnose primjenom postupaka utvrđenih u posebnim ugovornim aranžmanima i ocjenjuju se u skladu s podtočkom (b).

(d) Organizacija surađuje u istragama sa svakom drugom organizacijom koja znatno pridonosi informacijskoj sigurnosti vlastitih aktivnosti.

(e) Organizacija može integrirati taj sustav izvješćivanja s drugim sustavima izvješćivanja koje je već uvela.

IS.D.OR.220 Incidenti povezani s informacijskom sigurnošću — otkrivanje, odgovor i oporavak

(a) Na temelju rezultata procjene rizika provedene u skladu s točkom IS.D.OR.205 i ishoda postupanja s rizicima provedenog u skladu s točkom IS.D.OR.210, organizacija provodi mjere za otkrivanje incidenata i ranjivosti koje ukazuju na moguću pojavu neprihvatljivih rizika i koje bi mogle utjecati na sigurnost zračnog prometa. Te mjere omogućuju da organizacija:

1. identificira odstupanja od unaprijed utvrđenih osnovnih vrijednosti funkcionalne učinkovitosti;

2. aktivira upozorenja za primjenu odgovarajućih mjera odgovora u slučaju bilo kakvog odstupanja.

(b) Organizacija provodi mjere odgovora na sve uvjete događaja identificiranih u podtočki (a) koji mogu postati ili su postali incident povezan s informacijskom sigurnošću. Te mjere odgovora omogućuju da organizacija:

1. pokrene reakciju na upozorenja iz podtočke (a) podpodtočke 2. aktiviranjem unaprijed definiranih resursa i načina postupanja;

2. ograniči širenje napada i izbjegne potpuno ostvarenje scenarija prijetnje;

3. kontrolira zakazivanje zahvaćenih elemenata definiranih u točki IS.D.OR.205 podtočki (a).

(c) Organizacija provodi mjere čiji je cilj oporavak od incidenata povezanih s informacijskom sigurnošću, uključujući hitne mjere, po potrebi. Te mjere oporavka omogućuju da organizacija:

1. ukloni ili ograniči na prihvatljivu razinu uvjete koji su uzrokovali incident;

2. ostvari sigurno stanje zahvaćenih elemenata definiranih u točki IS.D.OR.205 podtočki (a) unutar vremena oporavka koje je prethodno odredila organizacija.

IS.D.OR.225 Odgovor na nalaze koje je prijavilo nadležno tijelo

(a) Nakon primitka obavijesti o nalazima koju je dostavilo nadležno tijelo, organizacija:

1. utvrđuje temeljni uzrok ili temeljne uzroke neusklađenosti i čimbenike koji tomu doprinose;

2. utvrđuje plan korektivnih mjera;

3. dokazuje korekciju neusklađenosti na način prihvatljiv nadležnom tijelu.

(b) Mjere iz podtočke (a) provode se u razdoblju dogovorenom s nadležnim tijelom.

IS.D.OR.230 Sustav vanjskog izvješćivanja o informacijskoj sigurnosti

(a) Organizacija primjenjuje sustav izvješćivanja o informacijskoj sigurnosti koji je u skladu sa zahtjevima utvrđenima u Uredbi (EU) br. 376/2014 i njezinim delegiranim i provedbenim aktima ako se ta uredba primjenjuje na nju.

(b) Ne dovodeći u pitanje obveze iz Uredbe (EU) br. 376/2014, organizacija osigurava da se nadležnom tijelu prijavljuje svaki incident ili ranjivost povezana s informacijskom sigurnošću koji mogu predstavljati znatan rizik za sigurnost zračnog prometa. Nadalje:

1. ako takav incident ili ranjivost utječe na zrakoplov ili povezani sustav ili sastavni dio, organizacija o tome također izvješćuje nositelja odobrenja projekta;

2. ako takav incident ili ranjivost utječe na sustav ili sastavni dio koji upotrebljava organizacija, ona o tome izvješćuje organizaciju odgovornu za projektiranje sustava ili sastavnog dijela.

(c) Organizacija izvješćuje o stanju iz podtočke (b) kako slijedi:

1. obavijest se dostavlja nadležnom tijelu i, ako je primjenjivo, nositelju odobrenja projekta ili organizaciji odgovornoj za projektiranje sustava ili sastavnog dijela čim organizacija bude upoznata s tim stanjem;

2. izvješće se dostavlja nadležnom tijelu i, ako je primjenjivo, nositelju odobrenja projekta ili organizaciji odgovornoj za projektiranje sustava ili sastavnog dijela što prije, ali najkasnije 72 sata od trenutka kad je organizacija upoznata s tim stanjem, osim ako to spriječe izvanredne okolnosti.

   Izvješće se sastavlja u obliku koji određuje nadležno tijelo i sadrži sve relevantne informacije o stanju koje je poznato organizaciji;

3. izvješće o daljnjim mjerama podnosi se nadležnom tijelu i, ako je primjenjivo, nositelju odobrenja projekta ili organizaciji odgovornoj za projektiranje sustava ili sastavnog dijela, i sadržava pojedinosti o mjerama koje je organizacija poduzela ili koje namjerava poduzeti kako bi se oporavila od incidenta i mjerama koje namjerava poduzeti kako bi spriječila slične incidente u vezi s informacijskom sigurnošću u budućnosti.

   Izvješće o daljnjim mjerama podnosi se čim se utvrde te mjere i sastavlja se u obliku koji odredi nadležno tijelo.

IS.D.OR.235 Ugovaranje aktivnosti upravljanja informacijskom sigurnošću

(a) Organizacija osigurava da su pri ugovaranju bilo kojeg dijela aktivnosti iz točke IS.D.OR.200 s drugim organizacijama ugovorene aktivnosti u skladu sa zahtjevima ove Uredbe i da organizacija s kojom je sklopljen ugovor radi pod njezinim nadzorom. Organizacija osigurava da se rizicima povezanima s ugovorenim aktivnostima upravlja na odgovarajući način.

(b) Organizacija osigurava da nadležno tijelo na zahtjev može imati pristup organizaciji s kojom je sklopljen ugovor kako bi se utvrdila kontinuirana usklađenost s primjenjivim zahtjevima utvrđenima u ovoj Uredbi.

IS.D.OR.240 Zahtjevi u vezi s osobljem

(a) Odgovorni rukovoditelj organizacije ili, u slučaju projektnih organizacija, rukovoditelj projektne organizacije, imenovan u skladu s Uredbom (EU) br. 748/2012 i Uredbom (EU) br. 139/2014 kako je navedeno u članku 2. točki 1. podtočkama (a) i (b) ove Uredbe, ima statutarnu ovlast osigurati financiranja i provedbe svih aktivnosti koje se zahtijevaju ovom Uredbom. Ta osoba mora:

   1. osigurati dostupnost svih potrebnih sredstava za ispunjavanje zahtjeva ove Uredbe;

   2. uspostaviti i promicati politiku informacijske sigurnosti iz točke IS.D.OR.200 podtočke (a) podpodtočke (1);

   3. pokazati osnovno razumijevanje ove Uredbe.

(b) Odgovorni rukovoditelj ili, u slučaju projektnih organizacija, rukovoditelj projektne organizacije imenuje osobu ili skupinu osoba za osiguravanje da organizacija ispunjava zahtjeve ove Uredbe i određuje opseg njihovih ovlasti. Ta osoba ili skupina osoba izravno odgovara odgovornom rukovoditelju ili, u slučaju projektnih organizacija, rukovoditelju projektne organizacije i mora imati odgovarajuće znanje, obrazovanje i iskustvo za izvršavanje svojih odgovornosti. U postupcima se određuje tko zamjenjuje određenu osobu u slučaju njezine dugotrajne odsutnosti.

(c) Odgovorni rukovoditelj ili, u slučaju projektnih organizacija, rukovoditelj projektne organizacije imenuje osobu ili skupinu osoba za upravljanje funkcijom praćenja usklađenosti iz točke IS.D.OR.200 podtočke (a) podpodtočke 12.

(d) Ako organizacija dijeli organizacijske strukture, politike, procese i postupke povezane s informacijskom sigurnošću s drugim organizacijama ili područjima aktivnosti u vlastitoj organizaciji koja nisu dio odobrenja ili izjave, odgovorni rukovoditelj ili, u slučaju projektnih organizacija, rukovoditelj projektne organizacije može povjeriti te aktivnosti zajedničkoj odgovornoj osobi.

U tom slučaju uspostavljaju se mjere koordinacije između odgovornog rukovoditelja organizacije ili, u slučaju projektnih organizacija, rukovoditelja projektne organizacije i zajedničke odgovorne osobe kako bi se osigurala odgovarajuća integracija upravljanja informacijskom sigurnošću unutar organizacije.

(e) Odgovorni rukovoditelj ili rukovoditelj projektne organizacije, ili zajednička odgovorna osoba iz podtočke (d), imaju statutarnu ovlast uspostaviti i održavati organizacijske strukture, politike, procese i postupke potrebne za primjenu točke IS.D.OR.200.

(f) Organizacija mora imati uspostavljen postupak kojim se osigurava da ima dovoljno osoblja za obavljanje aktivnosti obuhvaćenih ovim Prilogom.

(g) Organizacija mora imati uspostavljen postupak kojim se osigurava da osoblje iz podtočke (f) ima potrebnu stručnost za obavljanje svojih zadaća.

(h) Organizacija mora imati uspostavljen postupak kojim se osigurava da je osoblje upoznato s odgovornostima povezanima s dodijeljenim ulogama i zadaćama.

(i) Organizacija osigurava da su identitet i pouzdanost osoblja koje ima pristup informacijskim sustavima i podacima podložni zahtjevima ove Uredbe primjereno utvrđeni.

IS.D.OR.245 Vođenje evidencije

(a) Organizacija vodi evidenciju o svojim aktivnostima upravljanja informacijskom sigurnošću.

1. Organizacija osigurava arhiviranje i sljedivost sljedeće evidencije:

i. sva primljena odobrenja i sve povezane procjene rizika za informacijsku sigurnost u skladu s točkom IS.D.OR.200 podtočkom (e);

ii. ugovore za aktivnosti iz točke IS.D.OR.200 podtočke (a) podpodtočke 9.;

iii. evidenciju ključnih postupaka iz točke IS.D.OR.200 podtočke (d);

iv. evidenciju o rizicima utvrđenima u procjeni rizika iz točke IS.D.OR.205 i povezanim mjerama postupanja s rizicima iz točke IS.D.OR.210;

v. evidenciju o incidentima i ranjivostima povezanima s informacijskom sigurnošću prijavljenima u skladu sa sustavima izvješćivanja iz točaka IS D.OR.215 i IS.D.OR.230;

vi. evidenciju o događajima povezanima s informacijskom sigurnošću koje će možda trebati ponovno procijeniti kako bi se otkrili neotkriveni incidenti ili ranjivosti povezani s informacijskom sigurnošću.

2. Evidencija iz podpodtočke 1. podpodpodtočke i. čuva se najmanje pet godina nakon što odobrenje prestane važiti.

3. Evidencija iz podpodtočke 1. podpodpodtočke ii. čuva se najmanje pet godina nakon izmjene ili raskida ugovora.

4. Evidencija iz podpodtočke 1. podpodpodtočaka iii., iv. i v. čuva se najmanje pet godina.

5. Evidencija iz podpodtočke 1 podpodpodtočke vi. čuva se dok se ti događaji povezani s informacijskom sigurnošću ponovno ne ocijene u skladu s učestalošću utvrđenom u postupku koji je utvrdila organizacija.

(b) Organizacija vodi evidenciju o kvalifikacijama i iskustvu vlastitog osoblja uključenog u aktivnosti upravljanja informacijskom sigurnošću.

1. Evidencija o kvalifikacijama i iskustvu osoblja čuva se sve dok osoba radi za organizaciju i najmanje tri godine nakon što je osoba napustila organizaciju.

2. Članovima osoblja na njihov se zahtjev daje pristup njihovim pojedinačnim evidencijama. Osim toga, organizacija im na njihov zahtjev po napuštanju organizacije dostavlja presliku njihove osobne evidencije.

(c) Format evidencije mora biti određen u postupcima organizacije.

(d) Evidencija se čuva na način kojim se osigurava zaštita od oštećenja, preinake ili krađe, a informacije se po potrebi identificira u skladu s njihovih stupnjem tajnosti. Organizacija osigurava da se evidencija čuva na način kojim se osigurava integritet, autentičnost i odobren pristup.

IS.D.OR.250 Priručnik za upravljanje informacijskom sigurnošću (ISSM)

(a) Organizacija nadležnom tijelu stavlja na raspolaganje priručnik za upravljanje informacijskom sigurnošću (ISMM) i, ako je primjenjivo, sve povezane priručnike i postupke na koje se upućuje, koji sadržavaju:

1. izjavu koju je potpisao odgovorni rukovoditelj ili, u slučaju projektnih organizacija, rukovoditelj projektne organizacije, kojom se potvrđuje da će

organizacija u svakom trenutku postupati u skladu s ovim Prilogom i ISMM-om. Ako odgovorni rukovoditelj ili, u slučaju projektnih organizacija, rukovoditelj projektne organizacije nije glavni izvršni direktor (CEO) organizacije, tada taj glavni izvršni direktor supotpisuje izjavu;

2. titule, imena, dužnosti, odgovornosti i ovlasti osobe ili osoba iz točke IS.D.OR.240 podtočaka (b) i (c);
3. titulu, ime, dužnosti, odgovornosti i ovlasti zajedničke odgovorne osobe iz točke IS.D.OR.240 podtočke (d), ako je primjenjivo;
4. politiku informacijske sigurnosti organizacije iz točke IS.D.OR.200 podtočke (a) podpodtočke 1.;
5. opći opis broja i kategorija osoblja i uspostavljenog sustava za planiranje raspoloživosti osoblja kako je propisano točkom IS.D.OR.240;
6. titule, imena, dužnosti, odgovornosti i ovlasti ključnih osoba odgovornih za primjenu točke IS.D.OR.200, uključujući osobu ili osobe odgovorne za funkciju praćenja usklađenosti iz točke IS.D.OR.200 podtočke (a) podpodtočke 12.;
7. organigram koji prikazuje povezane lance odgovornosti za osobe iz podpodtočaka 2. i 6.;
8. opis sustava unutarnjeg izvješćivanja iz točke IS.D.OR.215;
9. postupke kojima se utvrđuje kako organizacija osigurava usklađenost s ovim dijelom, a posebno:
   i. dokumentaciju iz točke IS.D.OR.200 podtočke (c);
   ii. postupke kojima se definira kako organizacija kontrolira sve ugovorene aktivnosti iz točke IS.D.OR.200 podtočke (a) podpodtočke (9);
   iii. postupak izmjene ISMM-a definiran u podtočki (c);
10. popis trenutačno odobrenih alternativnih načina usklađivanja.

(b) Prvo izdanje ISMM-a odobrava se, a jedan primjerak zadržava nadležno tijelo. ISMM se izmjenjuje prema potrebi kako bi kontinuirano bio ažurni opis ISMS-a organizacije. Primjerak svih izmjena ISMM-a dostavlja se nadležnom tijelu.

(c) Izmjenama ISMM-a upravlja se u skladu s postupkom koji utvrđuje organizacija. Sve izmjene koje nisu obuhvaćene ovim postupkom te izmjene povezane s promjenama navedenima u točki IS.D.OR.255 podtočki (b) odobrava nadležno tijelo.

(d) Organizacija može integrirati ISMM s drugim priručnicima za upravljanje ili priručnicima koje pohranjuje, pod uvjetom da postoji jasno unakrsno upućivanje koje pokazuje koji dijelovi priručnika za upravljanje odgovaraju različitim zahtjevima sadržanima u ovom Prilogu.

IS.D.OR.255 Promjene sustava upravljanja informacijskom sigurnošću

(a) Promjenama ISMS-a može se upravljati i o njima obavijestiti nadležno tijelo provedbom postupka koji je razvila organizacija. Taj postupak odobrava nadležno tijelo.

(b) U pogledu promjena ISMS-a koje nisu obuhvaćene postupkom iz podtočke (a), organizacija podnosi zahtjev i dobiva odobrenje koje izdaje nadležno tijelo.

U pogledu tih promjena:

1. zahtjev se podnosi prije uvođenja bilo kakve takve promjene, kako bi nadležno tijelo moglo utvrditi kontinuiranu usklađenost s ovom Uredbom i, prema potrebi, izmijeniti certifikat organizacije i povezane uvjete odobrenja koji su mu priloženi;
2. organizacija nadležnom tijelu stavlja na raspolaganje sve informacije koje zatraži radi ocjene promjene;
3. promjena se provodi tek nakon primitka službenog odobrenja nadležnog tijela;
4. organizacija mora postupati u skladu s uvjetima koje je propisalo nadležno tijelo tijekom provedbe takvih promjena.

IS.D.OR.260 Kontinuirano poboljšavanje

(a) Organizacija procjenjuje, koristeći odgovarajuće pokazatelje uspješnosti, djelotvornost i zrelost ISMS-a. Ta se procjena provodi na temelju kalendara koji je unaprijed odredila organizacija ili nakon incidenta u vezi s informacijskom sigurnošću.

(b) Ako se nakon procjene provedene u skladu s podtočkom (a) utvrde nedostaci, organizacija poduzima potrebne mjere za poboljšanje kako bi osigurala da ISMS i dalje ispunjava primjenjive zahtjeve i održava rizike za informacijsku sigurnost na prihvatljivoj razini. Osim toga, organizacija ponovno ocjenjuje one elemente ISMS-a na koje utječu donesene mjere.