**PRILOG 1**

**DELEGIRANA REGULATIVA KOMISIJE (EU) 2022/1645**
**od 14. jula 2022. godine**
**o utvrđivanju pravila za primjenu Regulative (EU) 2018/1139 Evropskog parlamenta i Savjeta u vezi sa zahtjevima za upravljanje rizicima informacione bezbjednosti sa potencijalnim uticajem na sigurnost vazduhoplovstva za organizacije obuhvaćene regulativama Komisije (EU) br. 748/2012 i (EU) br. 139/2014 i o izmjeni regulative Komisije (EU) br. 748/2012 i (EU) br. 139/2014**

*Član 1*
**Predmet**

Ovom regulativom se utvrđuju zahtjevi koje treba da ispune organizacije iz člana 2 kako bi identifikovale i upravljale rizicima informacione bezbjednosti sa potencijalnim uticajem na sigurnost vazduhoplovstva, što bi moglo da utiče na sisteme informacione i komunikacione tehnologije i podatke koji se koriste u civilnom vazduhoplovstvu kako bi se otkrili informacioni bezbjednosni događaji i identifikovali oni koji se smatraju incidentima povezanim s informacionom bezbjednošću sa potencijalnim uticajem na vazduhoplovnu sigurnost i reagovanje na te incidente povezane sa informacionom bezbjednošću i oporavak od njih.

*Član 2*
**Područje primjene**

1. Ova Regulativa primjenjuje se na sljedeće organizacije:

(a) organizacije za proizvodnju i organizacije za projektovanje u skladu sa poddjelovima G i J odsjeka A Priloga I (Dio 21) Regulative (EU) br. 748/2012, osim organizacija za projektovanje i proizvodnju koje su isključivo uključene u projektovanje i/ili proizvodnju vazduhoplova ELA2 kako je definisano u članu 1(2), tački (j) Regulative (EU) br. 748/2012;
(b) operatore aerodroma i pružaoce usluga upravljanja platformom u skladu sa Prilogom III „Zahtjevi u vezi sa organizacijama (Dio ADR.OR)" Regulative (EU) br. 139/2014,
(c) organizacije za zemaljsko opsluživanje na koje se primjenjuje Delegirana regulativa Komisije (EU) 2025/20(*) koje:[1]
    (i) da bi pružile odgovarajuće usluge treba da prikupljaju, čuvaju, analiziraju ili na drugi način obrađuju podatke trećih strana/lica; ili
    (ii) operatorima vazduhoplova direktno dostavljaju podatke koji će se koristiti u operativne svrhe.

(*) Delegirana regulativa Komisije (EU) 2025/20 od 19. decembra 2024. godine o dopuni Regulative (EU) 2018/1139 Evropskog parlamenta i Savjeta utvrđivanjem zahtjeva za sigurno pružanje usluga zemaljskog opsluživanja i za organizacije koje ih pružaju".

2. Ovom regulativom ne dovode se u pitanje zahtjevi u pogledu informacione bezbjednosti i sajber bezbjednosti utvrđeni u tački 1.7 Priloga Sprovedbene regulative (EU) 2015/1998 i članu 14 Direktive (EU) 2016/1148.

*Član 3*
**Značenje izraza**

Za potrebe ove regulative primjenjuju se sljedeća značenja izraza:
(1) „informaciona bezbjednost" je očuvanje povjerljivosti, integriteta, autentičnosti i dostupnosti mrežnih i informacionih sistema;
(2) „informacioni bezbjednosni događaj" je identifikovani događaj u stanju sistema, usluge ili mreže koji ukazuje na moguće kršenje politike informacione bezbjednosti ili na otkaz kontrola informacione bezbjednosti ili prethodno nepoznatu situaciju koja može biti relevantna za informacionu bezbjednost;
(3) „incident" je bilo koji događaj koji ima negativni efekat na bezbjednost mrežnih i informacionih sistema; kako je definisano u članu 4(7) Direktive (EU) 2016/1148;
(4) „rizik informacione bezbjednosti" je rizik za organizacione operacije civilnog vazduhoplovstva, imovinu, pojedince i druge organizacije zbog potencijalnog događaja u području informacione bezbjednosti. Rizici informacione bezbjednosti povezani su s mogućnošću da će prijetnje iskoristiti ranjivosti informacione imovine ili grupe informacione imovine;
(5) „prijetnja" je potencijalna povreda informacione bezbjednosti koja je prisutna kada postoji subjekt, okolnost, radnja ili događaj koji bi mogli da prouzrokuju štetu;
(6) „ranjivost" je nedostatak ili slaba tačka u imovini ili sistemu, procedurama, projektu, sprovođenju ili mjerama informacione bezbjednosti koja bi se mogla iskoristiti i koja dovodi do kršenja politike informacione bezbjednosti.

*Član 4*
**Zahtjevi koji proizilaze iz drugih zakonodavnih akata Unije**

1. Ako organizacija iz člana 2 ispunjava bezbjednosne zahtjeve utvrđene u članu 14 Direktive (EU) 2016/1148 koji su ekvivalentni zahtjevima utvrđenim u ovoj regulativi, usklađenost sa tim bezbjednosnim zahtjevima smatra se usklađenošću sa zahtjevima utvrđenim u ovoj regulativi.

[1] Odredba se primjenjuje primjenjuje se od 27. marta 2031. godine.

2. Ako je organizacija iz člana 2 operator ili subjekt iz nacionalnih programa bezbjednosti civilnog vazduhoplovstva država članica utvrđenih u skladu s članom 10 Regulative (EZ) br. 300/2008 Evropskog parlamenta i Savjeta[2], zahtjevi informacione bezbjednosti iz tačke 1.7 Priloga Sprovedbene regulative (EU) 2015/1998 smatraju se ekvivalentni zahtjevima utvrđenim u ovoj regulativi, osim u pogledu tačke IS.D.OR.230 Priloga ove regulative koja se mora poštovati.
3. Komisija, nakon savjetovanja sa EASA-om i grupom za saradnju iz člana 11 Direktive (EU) 2016/1148 Komisija može da izda uputstva za procjenu ekvivalentnosti zahtjeva utvrđenih u ovoj regulativi i Direktivi (EU) 2016/1148.

*Član 5*

**Nadležni organ**

1. Nadležni organ za sertifikovanje i nadzor usklađenosti s ovom regulativom je:

(a) za organizacije iz člana 2 tačke (a), nadležni organ imenovan u skladu s Prilogom I (Dio 21) Regulative (EU) br. 748/2012;
(b) za organizacije iz člana 2 tačke (b), nadležni organ imenovan u skladu s Prilogom III (Dio ADR.OR) Regulative (EU) br. 139/2014,
(c) za organizacije iz člana 2 tačke (c) nadležni organ imanovan u skladu sa Prilogom (Dio-ARGH) Sprovedbene regulative Komisije (EU) br.2025/23 (*).[3]

---

(*) Sprovedbena regulativa Komisije (EU) 2025/23 od 19. decembra 2024. godine o utvrđivanju pravila za primjenu Regulative (EU) 2018/1139 Evropskog parlamenta i Savjeta u pogledu zahtjeva za nadzor usluga zemaljskog opsluživanja i organizacija koje ih pružaju".

2. Države članice mogu, za potrebe ove regulative, da imenuju nezavisni i autonomni subjekt za izvršavanje dodijeljene uloge i odgovornosti nadležnih organa iz stava 1. U tom slučaju, uspostavljaju se mjere koordinacije između tog subjekta i nadležnih organa, kako je navedeno u stavu 1, kako bi se obezbijedio djelotvoran nadzor nad svim zahtjevima koje organizacija mora da ispuni.

*Član 6*

**Izmjene i dopune Regulative (EU) br. 748/2012**

Prilog I (Dio 21) Regulative (EU) br. 748/2012 mijenja se kako slijedi:

(1) sadržaj se mijenja kako slijedi:
(a) nakon naslova 21.A.139 umeće se sljedeći naslov:

**„21.A.139A Sistem upravljanja informacionom bezbjednošću";**

(b) nakon naslova 21.A.239 umeće se sljedeći naslov:

**„21.A.239A Sistem upravljanja informacionom bezbjednošću ";**

(2) nakon tačke 21.A.139 umeće se tačka 21.A.139 A:

**„21.A.139A Sistem upravljanja informacionom bezbjednošću**

Pored sistema upravljanja proizvodnjom koji se zahtijeva tačkom 21.A.139, organizacija za proizvodnju dužna je da uspostavi, primjenjuje i održava sistem upravljanja informacionom bezbjednošću u skladu s Delegiranom regulativom Komisije (EU) 2022/1645(*) kako bi se obezbijedilo pravilno upravljanje rizicima informacione bezbjednosti koji mogu uticati na sigurnost vazduhoplovstva."

---

(*) Delegirana regulativa Komisije (EU) 2022/1645 od 14. jula 2022. godine o utvrđivanju pravila za primjenu Regulative (EU) 2018/1139 Evropskog parlamenta i Savjeta u pogledu zahtjeva za upravljanje rizicima informacione bezbjednosti koji mogu uticati na sigurnost vazduhoplovstva za organizacije obuhvaćene Regulativama Komisije (EU) br. 748/2012 i (EU) br. 139/2014 i o izmjeni Regulativa Komisije (EU) br. 748/2012 i (EU) br. 139/2014 (SL L 248, 26.9.2022., str. 18.). ";

(3) nakon tačke 21.A.239 umeće se tačka 21.A.239A:

**„21.A.239A Sistem upravljanja informacionom bezbjednošću**

Pored sistema upravljanja projektom koji se zahtijeva tačkom 21.A.239, organizacija za projektovanje dužna je da uspostavi, primjenjuje i održava sistem upravljanja informacionom bezbjednossću u skladu s Delegiranom Regulativom (EU) 2022/1645 kako bi se obezbijedilo pravilno upravljanje rizicima informacione bezbjednosti koji mogu uticati na sigurnost vazduhoplovstva.".

*Član 7*

**Izmjena Regulative (EU) br. 139/2014**

Prilog III (Part-ADR.OR) Regulative (EU) br. 139/2014 mijenja se kako slijedi:

(1) nakon tačke ADR.OR.D.005 umeće se tačka ADR.OR.D.005A:

**„ADR.OR.D.005A Sistem upravljanja informacionom bezbjednošću**

---

[2] Regulativa (EZ) br. 300/2008 Evropskog parlamenta i Savjeta od 11. marta 2008. godine o zajedničkim pravilima u oblasti bezbjednosti civilnog vazduhoplovstva i o ukidanju Regulative (EZ) br. 2320/2002 (OJ L 97, 9.4.2008, str.72)

[3] Odredba se primjenjuje primjenjuje se od 27. marta 2031. godine.

Operator aerodroma dužan je da uspostavi, primjenjuje i održava sistem upravljanja informacionom bezbjednošću u skladu sa Delegiranom Regulativom Komisije (EU) 2022/1645 (*) kako bi se obezbijedilo pravilno upravljanje rizicima informacione bezbjednosti koji mogu uticati na sigurnost vazduhoplovstva.

---

(*) Delegirana Regulativa Komisije (EU) 2022/1645 od 14. jula 2022. o utvrđivanju pravila za primjenu Regulative (EU) 2018/1139 Evropskog parlamenta i Savjeta u vezi sa zahtjevima za upravljanje rizicima informacione bezbjednosti koji mogu da utiču na sigurnost vazduhoplovstva za organizacije obuhvaćene Regulativama Komisije (EU) br. 748/2012 i (EU) br. 139/2014 i o izmjeni Regulativa Komisije (EU) br. 748/2012 i (EU) br. 139/2014 (SL L 248, 26.9.2022., str. 18.).";

(2) tačka ADR.OR.D.007 zamjenjuje se sljedećim:

**„ADR.OR.D.007 Upravljanje vazduhoplovnim podacima i vazduhoplovnim informacijama**

(a) U okviru svog sistema upravljanja, operator aerodroma primjenjuje i održava sistem upravljanja kvalitetom koji obuhvata sljedeće aktivnosti:
   (1) njegove aktivnosti u vezi sa vazduhoplovnim podacima;
   (2) njegove aktivnosti u vezi s pružanjem vazduhoplovnih informacija.

(b) U okviru svog sistema upravljanja, operator aerodroma uspostavlja sistem upravljanja bezbjednošću radi zaštite bezbjednosti operativnih podataka koje prima ili proizvodi ili upotrebljava, tako da pristup tim operativnim podacima imaju samo ovlašćena lica.

(c) U sistemu upravljanja bezbjednošću definišu se sljedeći elementi:
   (1) procedure koje se odnose na procjenu i ublažavanje rizika bezbjednosti podataka, praćenje i unapređivanje bezbjednosti, pregled bezbjednosti i dijeljenje iskustava;
   (2) sredstva projektovana za otkrivanje povreda bezbjednosti i za upozoravanje osoblja odgovarajućim bezbjednosnim upozorenjima;
   (3) sredstva za kontrolu posljedica povrede bezbjednosti i utvrđivanje akcija oporavka i procedura ublažavanja, kako bi se spriječilo njihovo ponavljanje.

(d) Operator aerodroma dužan je da obezbijedi bezbjednosnu provjeru svog osoblja u odnosu na bezbjednost vazduhoplovnih podataka.

(e) Aspektima povezanim s informacionom bezbjednošću upravlja se u skladu s tačkom ADR.OR.D.005A.";

(3) nakon tačke ADR.OR.F.045 umeće se tačka ADR.OR.F.045A:

**„ADR.OR.F.045A Sistem upravljanja informacionom bezbjednošću**

Organizacija odgovorna za pružanje AMS-a dužna je uspostavi, primjenjuje i održava sistem upravljanja informacionom bezbjednošću u skladu s Delegiranom Regulativom (EU) 2022/1645 kako bi se obezbijedilo pravilno upravljanje rizicima informacione bezbjednosti koji mogu uticati na sigurnost vazduhoplovstva."

*Član 8*

Ova regulativa stupa na snagu dvadesetog dana od dana objave u *Službenom listu Evropske unije*.

Primjenjuje se od 16. oktobra 2025. godine

Ova regulativa obavezujuća je u cjelini i neposredno se primjenjuje u svim državama članicama.

Sačinjeno u Briselu 14. jula 2022. godine

*Za Komisiju*
Predsjednica
Ursula VON DER LEJEN

PRILOG

**INFORMACIONA BEZBJEDNOST — ZAHTJEVI U VEZI S ORGANIZACIJAMA**
**[PART-IS.D.OR]**



**IS.D.OR.100 Područje primjene**

U ovom dijelu utvrđuju se zahtjevi koje treba da ispune organizacije iz člana 2 ove regulative.

**IS.D.OR.200 Sistem upravljanja informacionom bezbjednošću (ISMS)**

(a) Kako bi se ostvarili ciljevi utvrđeni u članu 1, organizacija uspostavlja, primjenjuje i održava sistem upravljanja informacionom bezbjednošću (ISMS) kojim se obezbjeđuje da organizacija:
  (1) uspostavlja politiku informacione bezbjednosti kojom se utvrđuju opšta načela organizacije u pogledu potencijalnog uticaja rizika informacione bezbjednosti na sigurnost vazduhoplovstva;
  (2) identifikuje i preispituje rizike informacione bezbjednosti u skladu sa tačkom IS.D.OR.205;
  (3) definiše i sprovodi mjere postupanja sa rizicima informacione bezbjednosti u skladu s tačkom IS.D.OR.210;
  (4) primjenjuje šemu internog izvještavanja o bezbjednosti informacija u skladu sa tačkom IS.D.OR.215;
  (5) definiše i sprovodi, u skladu sa tačkom IS.D.OR.220, potrebne mjere za otkrivanje događaja povezanih s informacionom bezbjednošću, identifikuje događaje koji se smatraju incidentima sa potencijalnim uticajem na sigurnost vazduhoplovstva, odgovara na te incidente i oporavlja se od njih;
  (6) implementira mjere koje je nadležni organ propisao kao neposrednu reakciju na incident ili ranjivost povezanu s informacionom bezbjednošću koja može uticati na sigurnost vazduhoplovstva;
  (7) preduzima odgovarajuću akciju, u skladu sa tačkom IS.D.OR.225, kako bi se otklonili nalazi (*findings*) koje je dao nadležni organ;
  (8) primjenjuje šemu eksternog izvještavanja u skladu s tačkom IS.D.OR.230 kako bi se nadležnom organu omogućilo da preduzme odgovarajuće mjere;
  (9) ispunjava zahtjeve iz tačke IS.D.OR.235 kada angažuje druge organizacije za bilo koji dio aktivnosti iz tačke IS.D.OR.200;
  (10) ispunjava zahtjeve u vezi sa osobljem utvrđene u skladu sa tačkom IS.D.OR.240;
  (11) ispunjava zahtjeve u vezi sa čuvanjem evidencije utvrđenim u skladu sa tačkom IS.D.OR.245;
  (12) prati usklađenost organizacije sa zahtjevima ove regulative i pruža povratne informacije o nalazima (*findings*) odgovornom rukovodiocu ili, u slučaju organizacija za projektovanje, odgovornom rukovodiocu organizacije za projektovanje kako bi se obezbijedilo djelotvorno sprovođenje korektivnih mjera;
  (13) Štiti, ne dovodeći u pitanje primjenljive zahtjeve za prijavljivanje incidenata, povjerljivost svih informacija koje je organizacija primila od drugih organizacija, u skladu sa njihovim stepenom osjetljivosti.

(b) Kako bi kontinuirano ispunjavala zahtjeve iz člana 1, organizacija sprovodi proces kontinuiranog unapređenja u skladu sa tačkom IS.D.OR.260.

(c) Organizacija, u skladu sa tačkom IS.D.OR.250, dokumentuje sve ključne procese, procedure, uloge i odgovornosti potrebne za usklađivanje sa tačkom IS.D.OR.200(a) i uspostavlja proces za izmjenu te dokumentacije. Promjenama tih procesa, procedura, uloga i odgovornosti upravlja se u skladu sa tačkom IS.D.OR.255.

(d) Procesi, procedure, uloge i odgovornosti koje je organizacija uspostavila radi usklađenosti sa tačkom IS.D.OR.200(a) odgovaraju prirodi i složenosti njenih aktivnosti, na osnovu procjene rizika informacione bezbjednosti svojstvenih tim aktivnostima, i mogu se uvrstiti u druge postojeće sisteme upravljanja koje organizacija već primjenjuje.

(e) Ne dovodeći u pitanje obavezu ispunjavanja zahtjeva za izvještavanje iz Regulative (EU) br. 376/2014 Evropskog parlamenta i Savjeta (1) i zahtjeve iz tačke IS.D.OR.200(a) (13), nadležni organ može organizaciji da izda odobrenje da se ne primjenjuju zahtjevi iz tačaka od (a) do (d) i povezanih zahtjeva iz tačaka od IS.D.OR.205 do IS.D.OR.260, ako dokaže, na zadovoljstvo tog organa, da njene aktivnosti, objekti i resursi, kao i usluge koje obavlja, pruža, prima i održava, ne predstavljaju ni njoj niti drugim organizacijama nikakve rizike informacione bezbjednosti sa potencijalnim uticajem na sigurnost vazduhoplovstva. Odobrenje se zasniva na dokumentovanoj procjeni rizika informacione bezbjednosti koju je sprovela organizacija ili treća strana u skladu sa tačkom IS.D.OR.205 i koju je pregledao i odobrio nadležni organ.

Nadležni organ će preispitati kontinuiranu važnost tog odobrenja nakon primjenljivog nadzornog ciklusa provjere i kad god se sprovedu promjene u području rada organizacije.

**IS.D.OR.205 Procjena rizika informacione bezbjednosti**

(a) Organizacija identifikuje sve svoje elemente koji mogu biti izloženi rizicima informacione bezbjednosti. To uključuje:
  (1) aktivnosti, objekte i resurse organizacije, kao i usluge koje organizacija obavlja, pruža, prima ili održava;
  (2) opremu, sisteme, podatke i informacije koji doprinose funkcionisanju elemenata navedenih u tački (1).

(b) Organizacija identifikuje interfejse koje ima sa drugim organizacijama i koji bi mogli dovesti do međusobne izloženosti rizicima informacione bezbjednosti.

(c) U pogledu elemenata i interfejsa iz tačaka (a) i (b), organizacija identifikuje rizike po informacionu bezbjednost sa potencijalnim uticajem na sigurnost vazduhoplovstva. Za svaki identifikovani rizik, organizacija je dužna da:
  (1) dodijeli nivo rizika u skladu s unaprijed definisanom klasifikacijom koju je utvrdila organizacija;
  (2) poveže svaki rizik i njegov nivo sa odgovarajućim elementom ili interfejsom utvrđenim u skladu sa tačkama (a) i (b).

U unaprijed definisanoj klasifikaciji iz tačke (1) uzima se u obzir potencijalna pojava scenarija prijetnje i ozbiljnost njegovih posljedica po sigurnost. Na osnovu te klasifikacije i uzimajući u obzir da li organizacija ima strukturisan i ponovljiv proces upravljanja rizicima za operacije, organizacija može da utvrdi je li rizik prihvatljiv ili je s njim potrebno postupati u skladu sa tačkom IS.D.OR.210.
Kako bi se olakšala međusobna uporedivost procjene rizika, pri dodjeljivanju nivoa rizika u skladu sa tačkom (1) uzimaju se u obzir relevantne informacije prikupljene u koordinaciji s organizacijama iz tačke (b).

(d) Organizacija pregleda i ažurira procjenu rizika sprovedenu u skladu sa tačkama (a), (b) i (c) u bilo kojoj od sljedećih situacija:
  (1) ako je došlo do promjene elemenata u zavisnosti od rizika informacione bezbjednosti;
  (2) ako jedo promjene u interfejsima između organizacije i drugih organizacija ili u rizicima koje su prijavile druge organizacije;
  (3) ako je do promjene informacija ili znanja koji se koriste za identifikaciju, analizu i klasifikaciju rizika;
  (4) ako su izvučene pouke na osnovu analize incidenata povezanih s informacionom bezbjednošću.

**IS.D.OR.210 Postupanje sa rizicima informacione bezbjednosti**

(a) Organizacija razvija mjere za otklanjanje neprihvatljivih rizika identifikovanih u skladu sa tačkom IS.D.OR.205, blagovremeno ih sprovodi i provjerava njihovu kontinuiranu efektivnost. Te mjere omogućuju da organizacija:
  (1) kontroliše okolnosti koje doprinose efektivnoj pojavi scenarija prijetnje;
  (2) ublaži posljedice na sigurnost vazduhoplovstva povezane sa realizacijom scenarija prijetnje;
  (3) izbjegava rizike.

Te mjere ne smiju da uvedu nove potencijalne neprihvatljive rizike po sigurnost vazduhoplovstva.

(b) Lice iz tačke IS.D.OR.240 tačaka (a) i (b) i drugo uključeno osoblje organizacije obavještavaju se o ishodu procjene rizika koja je sprovedena u skladu sa tačkom IS.D.OR.205, odgovarajućim scenarijima prijetnji i mjerama koje treba sprovesti.

Organizacija obavještava i organizacije sa kojima ima interfejs u skladu sa tačkom IS.D.OR.205(b) o svim rizicima koji su zajednički objema organizacijama.

**IS.D.OR.215 Šema internog izvještavanja o informacionoj bezbjednosti**

(a) Organizacija uspostavlja šemu internog izvještavanja radi prikupljanja i ocjene događaja povezanih sa informacionom bezbjednošću, uključujući one koje treba prijaviti u skladu sa tačkom IS.D.OR.230.

(b) Ta šema i proces iz tačke IS.D.OR.220 omogućuju da organizacija:
  (1) Identifikuje koji se događaji, prijavljeni u skladu sa tačkom (a), smatraju incidentima ili ranjivostima povezanim s informacionom bezbjednošću koji potencijalno mogu uticati na sigurnost vazduhoplovstva;
  (2) identifikuje uzroke i faktore koji doprinose nastanku incidenata i ranjivosti povezanih s informacionom bezbjednošću, utvrđenih u skladu sa tačkom 1 i rješava ih u okviru procesa upravljanja rizicima informacione bezbjednosti u skladu sa tačkama IS.D.OR.205 i IS.D.OR.220;
  (3) obezbjeđuje ocjenu svih poznatih relevantnih informacija koje se odnose na incidente i ranjivosti povezane s informacionom bezbjednošću, koje su identifikovane u skladu s tačkom 1;
  (4) obezbjeđuje primjenu metode za internu distribuciju informacija prema potrebi.

(c) Svaka ugovorena organizacija koja organizaciju može da izloži rizicima informacione bezbjednosti sa potencijalnim uticajem na sigurnost vazduhoplovstva dužna je da organizaciji prijavi događaje povezane s informacionom bezbjednošću. Te prijave podnose se primjenom procedura utvrđenih u posebnim ugovornim aranžmanima i ocjenjuju se u skladu s tačkom (b).

(d) Organizacija sarađuje u istragama sa svim drugim organizacijama koje značajno doprinose informacionoj bezbjednosti sopstvenih aktivnosti.

(e) Organizacija može da uvrsti šemu izvještavanja s drugim šemama izvještavanja koje je već sprovela.

**IS.D.OR.220 Incidenti povezani s informacionom bezbjednošću — otkrivanje, odgovor i oporavak**

(a) Na osnovu rezultata procjene rizika koja je sprovedena u skladu s tačkom IS.D.OR.205 i rezultata postupanja s rizicima koje je sprovedeno u skladu sa tačkom IS.D.OR.210, organizacija sprovodi mjere za otkrivanje incidenata i ranjivosti koje ukazuju na potencijalnu pojavu neprihvatljivih rizika i koje bi mogle uticati na sigurnost vazduhoplovstva. Te mjere omogućuju da organizacija:
  (1) identifikuje odstupanja od unaprijed utvrđenih osnovnih vrijednosti funkcionalnih performansi;
  (2) aktivira upozorenja za pokretanje odgovarajućih mjera odgovora, u slučaju bilo kakvog odstupanja.

(b) Organizacija sprovodi mjere sa ciljem da odgovori na sve uslove događaja koji su identifikovani u tački (a) koji mogu postati ili su već postali incident povezan s informacionom bezbjednošću. Te mjere odgovora omogućuju da organizacija:
  (1) pokrene reakciju na upozorenja iz tačke (a)(2) aktiviranjem unaprijed definisanih resursa i toka radnji;
  (2) ograniči širenje napada i izbjegne potpunu realizaciju scenarija prijetnje;
  (3) kontroliše način otkaza zahvaćenih elemenata definisanih u tački IS.D.OR.205(a).
(c) Organizacija sprovodi mjere čiji je cilj oporavak od incidenata povezanih s informacionom bezbjednošću, uključujući mjere u slučaju nužde, po potrebi. Te mjere oporavka omogućuju da organizacija:
  (1) ukloni stanje koji je dovelo do incidenta, ili da ga ograniči na podnošljivi nivo;
  (2) ostvari sigurno stanje zahvaćenih elemenata definisanih u tački IS.D.OR.205(a) u okviru vremena oporavka koji je prethodno odredila organizacija.

**IS.D.OR.225 Odgovor na nalaze nadležnog organa**

(a) Nakon prijema obavještenja o nalazima (*fidings*) koje je dostavio nadležni organ, organizacija:
  (1) utvrđuje osnovni uzrok ili uzroke neusklađenosti i faktore koji tome doprinose;
  (2) utvrđuje plan korektivnih mjera;
  (3) dokazuje korekciju neusklađenosti na način prihvatljiv nadležnom organu.
(b) Mjere iz tačke (a) sprovode se u periodu dogovorenom sa nadležnim organom.

**IS.D.OR.230 Šema eksternog izvještavanja o informacionoj bezbjednosti**

(a) Organizacija primjenjuje šemu izvještavanja o informacionoj bezbjednosti koja je u skladu sa zahtjevima utvrđenim u Regulativi (EU) br. 376/2014 i njenim delegiranim i sprovedbenim aktima, ako se ta regulativa primjenjuje na organizaciju.
(b) Ne dovodeći u pitanje obaveze iz Regulative (EU) br. 376/2014, organizacija obezbjeđuje da se nadležnom organu prijavljuje svaki incident ili ranjivost povezana s informacionom bezbjednošću koji mogu predstavljati značajan rizik za sigurnost vazduhoplovstva. Pored toga:
  (1) ako takav incident ili ranjivost utiče na vazduhoplov ili povezani sistem ili komponentu, organizacija o tome takođe izvještava nosioca odobrenja projekta;
  (2) ako takav incident ili ranjivost utiče na sistem ili komponentu koji koristi organizacija, ona o tome izvještava organizaciju koja je odgovorna za projektovanje sistema ili komponente.
(c) Organizacija izvještava o uslovima iz tačke (b) kako slijedi:
  (1) obavještenje se dostavlja nadležnom organu i, ako je primjenljivo, imaocu odobrenja projekta ili organizaciji koja je odgovorna za projektovanje sistema ili komponente čim organizaciji stanje bude poznato;
  (2) izvještaj se dostavlja nadležnom organu i, ako je primjenljivo, imaocu odobrenja projekta ili organizaciji koja je odgovorna za projektovanje sistema ili komponente što prije, u vremenskom intervalu ne dužem od 72 sata od trenutka kada je stanje poznato organizaciji, izuzev ukoliko to sprječavaju okolnosti.

  Izvještaj se sastavlja u obliku koji određuje nadležni organ i sadrži sve relevantne informacije o stanju koje je poznato organizaciji;
  (3) Izvještaj o pratećim aktivnostima podnosi se nadležnom organu i, ako je primjenljivo, imaocu odobrenja projekta ili organizaciji odgovornoj za projektovanje sistema ili komponente, i sadrži detaljne radnje koje je organizacija preduzela ili koje namjerava da preduzme kako bi se oporavila od incidenta i o mjerama koje namjerava da preduzme kako bi spriječila slične incidente u vezi s informacionom bezbjednošću u budućnosti.

  Izvještaj o pratećim aktivnostima podnosi se čim se te mjere utvrde i izrađuje se u obliku koji odredi nadležni organ.

**IS.D.OR.235 Ugovaranje aktivnosti upravljanja informacionom bezbjednošću**

(a) Organizacija obezbjeđuje da su prilikom ugovaranja bilo kojeg dijela aktivnosti iz tačke IS.D.OR.200 drugim organizacijama, ugovorene aktivnosti usklađene sa zahtjevima ove regulative i da ugovorene organizacije djeluju pod njenim nadzorom. Organizacija obezbjeđuje da se rizicima povezanim s ugovorenim aktivnostima upravlja na odgovarajući način.
(b) Organizacija obezbjeđuje da nadležni organ može, na zahtjev, imati pristup ugovorenoj organizaciji kako bi se utvrdila kontinuirana usklađenost sa primjenljivim zahtjevima utvrđenima u ovoj regulativi.

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

(a) Odgovorni rukovodilac organizacije ili, u slučaju organizacija za projektovanje, rukovodilac organizacije za projektovanje, imenovan u skladu s Regulativom (EU) br. 748/2012 i Regulativom (EU) br. 139/2014, kako je navedeno u tačkama 1(a) i (b) člana 2 ove regulative, ima korporativno ovlašćenje da obezbijedi da se sve aktivnosti koje se zahtijevaju ovom regulativom mogu finansijski obezbijediti i sprovesti. To lice mora da:
  (1) obezbijedi da su na raspolaganju sva potrebna sredstva za ispunjavanje zahtjeva ove regulative;
  (2) uspostavi i promoviše politiku informacione bezbjednosti iz tačke IS.D.OR.200(a)(1);
  (3) pokaže osnovno razumijevanje ove regulative.
(b) Odgovorni rukovodilac ili, u slučaju organizacija za projektovanje, rukovodilac organizacije za projektovanje imenuje lice ili grupu lica kako bi se obezbijedilo da organizacija ispunjava zahtjeve ove regulative i definiše obim njihovih ovlašćenja. To lice ili grupa lica direktno odgovara/ju odgovornom rukovodiocu ili, u slučaju organizacija za projektovanje, rukovodiocu

organizacije za projektovanje i mora da ima/ju odgovarajuće znanje, obrazovanje i iskustvo za izvršavanje svojih odgovornosti. U procedurama se određuje ko zamjenjuje određeno lice u slučaju njegovog dužeg odsustva.

(c) Odgovorni rukovodilac ili, u slučaju organizacija za projektovanje, rukovodilac organizacije za projektovanje, imenuje lice ili grupu lica za upravljanje funkcijom praćenja usklađenosti iz tačke IS.D.OR.200(a)(12).

(d) Ako organizacija dijeli organizacione strukture, politike, procese i procedure povezane s informacionom bezbjednošću sa drugim organizacijama ili područjima aktivnosti u sopstvenoj organizaciji koja nisu dio odobrenja ili izjave, odgovorni rukovodilac ili, u slučaju organizacija za projektovanje, rukovodilac organizacije za projektovanje može da delegira te aktivnosti zajedničkom odgovornom licu.

U tom slučaju, uspostavljaju se mjere koordinacije između odgovornog rukovodioca organizacije ili, u slučaju organizacija za projektovanje, rukovodioca organizacije za projektovanje i zajedničkog odgovornog lica kako bi se obezbijedila odgovarajuća integracija upravljanja informacionom bezbjednošću unutar organizacije.

(e) Odgovorni rukovodilac ili rukovodilac organizacije za projektovanje, ili zajedničko odgovorno lice iz tačke (d), ima korporativno ovlašćenje da uspostavi i održava organizacione strukture, politike, procese i procedure potrebne za primjenu tačke IS.D.OR.200.

(f) Organizacija mora da ima uspostavljen proces kojim se obezbjeđuje da ima dovoljno osoblja za obavljanje aktivnosti obuhvaćenih ovim Prilogom.

(g) Organizacija mora da ima uspostavljen proces kojim se obezbjeđuje da osoblje iz tačke (f) ima potrebnu stručnost za obavljanje svojih zadataka.

(h) Organizacija mora da ima uspostavljen proces kojim se obezbjeđuje da je osoblje upoznato s odgovornostima povezanim sa dodijeljenim ulogama i zadacima.

(i) Organizacija obezbjeđuje da su identitet i pouzdanost osoblja koje ima pristup informacionim sistemima i podacima u skladu sa zahtjevima ove regulative adekvatno definisani.

**IS.D.OR.245 Vođenje evidencije**

(a) Organizacija vodi evidenciju o svojim aktivnostima upravljanja informacionom bezbjednošću.

(1) Organizacija obezbjeđuje da se arhiviraju i prate sljedeće evidencije:

(i) sva primljena odobrenja i sve povezane procjene rizika informacione bezbjednosti u skladu sa tačkom IS.D.OR.200(e);

(ii) ugovore za aktivnosti iz tačke IS.D.OR.200(a)(9);

(iii) evidenciju ključnih procesa iz tačke IS.D.OR.200(d);

(iv) evidenciju o rizicima utvrđenim u procjeni rizika iz tačke IS.D.OR.205 i povezanim mjerama postupanja sa rizicima iz tačke IS.D.OR.210;

(v) evidenciju o incidentima i ranjivostima povezanima s informacionom bezbjednošću koji su prijavljeni u skladu sa šemama izvještavanja iz tačaka IS.D.OR.215 i IS.D.OR.230;

(vi) evidenciju o događajima povezanim s informacionom bezbjednošću koje će možda biti potrebno ponovo procijeniti kako bi se ustanovili neotkriveni incidenti ili ranjivosti informacione bezbjednosti.

(2) Evidencije iz tačke (1)(i) čuvaju se najmanje pet godina nakon prestanka važenja odobrenja.

(3) Evidencije iz tačke (1)(ii) čuvaju se najmanje pet godina nakon izmjene ili raskida ugovora.

(4) Evidencije iz tačaka (1)(iii), (iv) i (v) čuvaju se najmanje pet godina.

(5) Evidencije iz tačke (1)(vi) čuvaju se dok se događaji povezani s informacionom bezbjednošću ponovo ne procijene u skladu sa periodičnošću koja je utvrđena procedurom koju je definisala organizacija.

(b) Organizacija vodi evidenciju o kvalifikacijama i iskustvu svog osoblja uključenog u aktivnosti upravljanja informacionom bezbjednošću.

(1) Evidencije o kvalifikacijama i iskustvu osoblja čuvaju se sve dok je to lice radno angažovano u organizaciji i najmanje tri godine nakon što je lice napustilo organizaciju.

(2) Članovi osoblja, na njihov zahtjev, dobijaju pristup svojim pojedinačnim evidencijama. Osim toga, organizacija im, na njihov zahtjev, po napuštanju organizacije, dostavlja kopiju njihovih ličnih evidencija.

(c) Format evidencije mora se definisati u procedurama organizacije.

(d) Evidencije se čuvaju na način kojim se obezbjeđuje zaštita od oštećenja, promjene ili krađe, a informacije se, po potrebi, identifikuju u skladu sa njihovim stepenom tajnosti. Organizacija obezbjeđuje da se evidencije čuvaju na način kojim se obezbjeđuje integritet, autentičnost i ovlašćen pristup.

**IS.D.OR.250 Priručnik za upravljanje informacionom bezbjednošću (ISSM)**

(a) Organizacija nadležnom organu stavlja na raspolaganje priručnik za upravljanje informacionom bezbjednošću (ISMM) i, ako je primjenljivo, sve povezane priručnike i procedure na koje se poziva, koji sadrže:

(1) potpisanu izjavu odgovornog rukovodioca ili, u slučaju organizacija za projektovanje, rukovodioca organizacije za projektovanje, kojom se potvrđuje da će organizacija u svakom trenutku postupati u skladu s ovim Prilogom i ISMM-om. Ako odgovorni rukovodilac ili, u slučaju organizacija za projektovanje, rukovodilac organizacije za projektovanje nije glavni izvršni direktor (CEO) organizacije, tada glavni (izvršni) direktor takođe potpisuje izjavu, pored rukovodioca organizacije;

(2) zvanja, imena, dužnosti, odgovornosti i ovlašćenja lica ili licâ iz tačke IS.D.OR.240(b) i (c);

(3) zvanje, ime, dužnosti, odgovornosti i ovlašćenja zajedničkog odgovornog lica iz tačke IS.D.OR.240(d), ako je primjenljivo;

(4) politiku informacione bezbjednosti organizacije iz tačke IS.D.OR.200(a)(1);
(5) opšti opis broja i kategorija osoblja i uspostavljenog sistema za planiranje raspoloživosti osoblja kako je propisano tačkom IS.D.OR.240;
(6) zvanja, imena, dužnosti, odgovornosti i ovlašćenja ključnih osoba odgovornih za primjenu tačke IS.D.OR.200, uključujući lice ili lica odgovornih za funkciju praćenja usklađenosti iz tačke IS.D.OR.200(a)(12);
(7) organizacinu šemu koja prikazuje povezanost i odgovornosti lica iz tačaka (2) i (6);
(8) šematski prikaz internog izvještavanja iz tačke IS.D.OR.215;
(9) procedure kojima se utvrđuje kako organizacija obezbjeđuje usklađenost s ovim dijelom, a posebno:
    (i) dokumentaciju iz tačke IS.D.OR.200(c);
    (ii) procedure kojima se definiše kako organizacija kontroliše sve ugovorene aktivnosti iz tačke IS.D.OR.200(a)(9);
    (iii) proceduru izmjene ISMM-a koja je definisana u tački (c);
(10) detalje o trenutno odobrenim alternativnim načinima usklađivanja.

(b) Prvo izdanje ISMM-a odobrava, a jedan primjerak zadržava nadležni organ. Odobrenje nije potrebno za deklarisane organizacije. ISMM se izmjenjuje prema potrebi kako bi postojao ažurirani opis ISMS-a organizacije. Primjerak svih izmjena ISMM-a dostavlja se nadležnom organu.
(c) Izmjenama ISMM-a upravlja se u skladu s procedurom koju utvrđuje organizacija. Sve izmjene koje nisu obuhvaćene ovom procedurom i sve izmjene povezane s promjenama navedenim u tački IS.D.OR.255(b) odobrava nadležni organ. Odobrenje nije potrebno za deklarisane organizacije.
(d) Organizacija može da integriše ISMM s drugim priručnicima za upravljanje ili priručnicima koje posjeduje, pod uslovom da postoji jasno unakrsno pozivanje koje ukazuje koji djelovi priručnika ili priručnika za upravljanje odgovaraju različitim zahtjevima iz ovog Priloga.

**IS.D.OR.255 Promjene sistema upravljanja informacionom bezbjednošću**

(a) Promjenama ISMS-a može se upravljati i o njima se može obavijestiti nadležni organ procedurom koju je razvila organizacija. Tu proceduru odobrava nadležni organ, osim za deklarisane organizacije.
(b) U vezi sa promjenama ISMS-a koje nisu obuhvaćene procedurom iz tačke (a), organizacija podnosi zahtjev, i dobija odobrenje koje izdaje nadležni organ osim za deklarisane organizacije za koje odobrenje nije potrebno.

U vezi sa tim promjenama:

(1) zahtjev se podnosi prije uvođenja bilo kakve promjene, kako bi nadležni organ mogao da utvrdi kontinuiranu usklađenost s ovom regulativom i da, prema potrebi, izmijeni sertifikat organizacije i povezane uslove odobrenja koji su mu priloženi;
(2) organizacija nadležnom organu stavlja na raspolaganje sve informacije koje zatraži radi ocjene promjene;
(3) promjena se sprovodi tek nakon prijema službenog odobrenja nadležnog organa, osim kod deklarisanih organizacija koje mogu bez odlaganja sprovesti promjenu.
(4) organizacija postupa u skladu s uslovima koje je propisao nadležni organ tokom sprovođenja takvih promjena.

**IS.D.OR.260 Kontinuirano unapređivanje**

(a) Organizacija procjenjuje efektivnost i sposobnost ISMS-a koristeći odgovarajuće indikatore efikasnosti. Ta se procjena sprovodi shodno unaprijed definisanom godišnjem planu koji je odredila organizacija ili nakon incidenta u vezi s informacionom bezbjednošću.
(b) Ako se nakon procjene koja je sprovedena u skladu s tačkom (a) utvrde nedostaci, organizacija preduzima potrebne mjere za unapređenje kako bi obezbijedila da ISMS i dalje ispunjava primjenljive zahtjeve i održava rizike informacione bezbjednosti na prihvatljivom nivou. Osim toga, organizacija ponovo procjenjuje one elemente ISMS-a na koje utiču donešene mjere.