|  |  |  |
| --- | --- | --- |
| **Republika e Kosovës**  Republika Kosova  Republic of Kosovo |  | **Autoriteti i Aviacionit Civil i Kosovës**  Autoritet Civilnog Vazduhoplovstva Kosova  Civil Aviation Authority of Kosovo |
|  | | |
|  | | |

**RREGULLORE (AAC) NR. XX/2025 E CILA PËRCAKTON RREGULLAT PËR ZBATIMIN E RREGULLORES (AAC) NR. 05/2020 NË LIDHJE ME KËRKESAT PËR MENAXHIMIN E RREZIQEVE TË SIGURISË SË INFORMACIONIT ME NJË NDIKIM TË MUNDSHËM NË SIGURINË E AVIACIONIT PËR ORGANIZATAT E MBULUARA NGA RREGULLORET (AAC) NR. 06/2015 DHE (AAC) NR. 17/2017 DHE QË NDRYSHON RREGULLORET (AAC) NR. 06/2015 DHE (AAC) NR. 17/2017**

**REGULATION (CAA) NO. XX/2025 LAYING DOWN RULES FOR THE APPLICATION OF REGULATION (CAA) NO. 05/2020 AS REGARDS REQUIREMENTS FOR THE MANAGEMENT OF INFORMATION SECURITY RISKS WITH A POTENTIAL IMPACT ON AVIATION SAFETY FOR ORGANISATIONS COVERED BY REGULATIONS (CAA) NO. 06/2015 AND (CAA) NO. 17/2017 AND AMENDING REGULATIONS (CAA) NO. 06/2015 AND (CAA) NO. 17/2017**

**UREDBA (ACV) BR. XX/2025 O UTVRĐIVANJU PRAVILA ZA PRIMENU UREDBE (ACV) BR. 05/2020 U POGLEDU ZAHTEVA ZA UPRAVLJANJE RIZICIMA INFORMACIONE BEZBEDNOSTI KOJI MOGU IMATI UTICAJ NA BEZBEDNOST VAZDUŠNOG SAOBRAĆAJA ZA ORGANIZACIJE OBUHVAĆENE UREDBAMA (ACV) BR. 06/2015 I (ACV) BR. 17/2017, KAO I O IZMENAMA I DOPUNAMA UREDBI (ACV) BR. 06/2015 I (ACV) BR. 17/2017**

|  |  |  |
| --- | --- | --- |
| Drejtori i Përgjithshëm i Autoritetit të Aviacionit Civil të Republikës së Kosovës,  Në mbështetje të neneve 21.2, 44, 61.2, 67, të Ligjit Nr. 03/L-051 për Aviacionin Civil (“Gazeta Zyrtare e Republikës së Kosovës”, Viti III, Nr. 28, datë 4 qershor 2008), i ndryshuar me Ligjin Nr. 08/L-063 për ndryshimin dhe plotësimin e ligjeve që kanë të bëjnë me racionalizimin dhe vendosjen e vijave llogaridhënëse të Agjencive të Pavarura,  Duke marrë parasysh,  Detyrimet ndërkombëtare të Republikës së Kosovës ndaj Marrëveshjes Shumëpalëshe për Themelimin e Hapësirës së Përbashkët Evropiane të Aviacionit (në tekstin e mëtejmë “Marrëveshja HPEA”) që nga hyrja e saj e përkohshme në fuqi për Kosovën më 10 tetor 2006,  Rregulloren (AAC) Nr. 05/2020 për rregullat e përbashkëta në fushën e aviacionit civil dhe themelimin e agjencisë së Bashkimit Evropian për sigurinë e aviacionit dhe ndryshimin e Rregullores (AAC) Nr. 10/2015 dhe shfuqizimin e Rregullores (AAC) Nr. 11/2009, Rregullores (AAC) Nr. 03/2009 dhe Rregullores (AAC) Nr. 6/2009,  Rregulloren (AAC) Nr. 17/2017 për Dispozitat dhe procedurat administrative në lidhje me aerodromet, e ndryshuar,  Nxjerr këtë:  **Rregullore (AAC) nr. XX/2025**  **e cila përcakton rregullat për zbatimin e Rregullores (AAC) nr. 05/2020 në lidhje me kërkesat për menaxhimin e rreziqeve të sigurisë së informacionit me një ndikim të mundshëm në sigurinë e aviacionit për organizatat e mbuluara nga Rregulloret (AAC) nr. 06/2015 dhe (AAC) nr. 17/2017 dhe që ndryshon Rregulloret (AAC) nr. 06/2015 dhe (AAC) nr. 17/2017**  **Neni 1**  **Qëllimi**   1. Qëllimi i kësaj Rregulloreje transpozimi I pjesshëm i Rregullores Deleguese të Komisionit (BE) Nr. 2022/1645 e 14 korrikut 2022 që përcakton rregullat për zbatimin e Rregullores (BE) 2018/1139 të Parlamentit Evropian dhe të Këshillit, në lidhje me kërkesat për menaxhimin e rreziqeve të sigurisë së informacionit me një ndikim të mundshëm në sigurinë e aviacionit për organizatat e mbuluara nga Rregulloret e Komisionit (BE) Nr. 748/2012 dhe (BE) Nr. 139/2014 dhe që ndryshon Rregulloret e Komisionit (BE) Nr. 748/2012 dhe (BE) Nr. 139/2014 në rendin e brendshëm juridik të Republikës së Kosovës. 2. Kjo Rregullore përcakton kërkesat që duhen përmbushur nga organizatat e referuar në nenin 2 me qëllim që të identifikohen dhe menaxhohen rreziqet e sigurisë së informacionit me ndikim të mundshëm në sigurinë e aviacionit e të cilat mund të ndikojnë në sistemet dhe të dhënat e teknologjisë së informacionit dhe komunikimit të cilat përdoren për qëllime të aviacionit civil dhe për të zbuluar ngjarjet e sigurisë së informacionit dhe për të identifikuar ato të cilat konsiderohen incidente të sigurisë së informacionit me ndikim të mundshëm në sigurinë e aviacionit dhe për të reaguar ndaj tyre, si dhe për t’u rikuperuar nga ato incidente të sigurisë së informacionit.   **Neni 2**  **Fushëveprimi**  1. Kjo Rregullore zbatohet për organizatat në vijim:  (a) Organizatat prodhuese dhe projektuese që janë subjekt i Nënpjesëve G dhe J të Seksionit A të Shtojcës 1 (Pjesa 21) të Rregullores (AAC) Nr. 06/2015 , përveç organizatave projektuese dhe prodhuese të cilat janë të përfshira në projektimin/ose prodhimin vetëm të mjetit ajror ELA2 siç përcaktohet në nenin 1(2), pika (j) e Rregullores (AAC) nr. 06/2015;  (b) operatorët e aerodromeve dhe ofruesit e shërbimit të menaxhimit të platformës që i nënshtrohen Shtojcës III 'Pjesa Kërkesat Organizative' (Pjesa-ADR.OR)' së Rregullores (AAC) Nr. 17/2017.  2. Kjo Rregullore nuk paragjykon kërkesat e sigurisë së informacionit dhe të sigurisë kibernetike të përcaktuara në pikën 1.7 të Shtojcës së Rregullores (MPB) nr. 04/2017 dhe në Rregulloren Nr. 68(ARKEP) mbi Sigurinë dhe Funksionimin e Duhur të Rrjeteve dhe/ose Shërbimeve të Komunikimeve Elektronike.  **Neni 3**  **Përkufizimet**  Për qëllime të kësaj Rregulloreje, do të zbatohen përkufizimet në vijim:  (1) “siguria e informacionit” nënkupton ruajtjen e konfidencialitetit, integritetit, autenticitetit dhe disponueshmërisë së rrjetit dhe sistemeve të informacionit;  (2) ‘Ngjarje e sigurisë së informacionit’ nënkupton një ndodhi të identifikuar në gjendjen e sistemit, shërbimit ose rrjetit e cila tregon një shkelje të mundshme të politikës së sigurisë së informacionit ose një dështim të kontrolleve të sigurisë së informacionit, apo një situatë të panjohur më parë e cila mund të jetë e rëndësishme për sigurinë e informacionit;  (3) ‘incident’ do të thotë çfarëdo ngjarje që ka një efekt negativ në sigurinë e sistemeve të rrjetit dhe informacionit siç përcaktohet në Rregulloren Nr. 68(ARKEP) mbi Sigurinë dhe Funksionimin e Duhur të Rrjeteve dhe/ose Shërbimeve të Komunikimeve Elektronike;  (4) ‘rrezik i sigurisë së informacionit’ nënkupton rrezikun për operacionet organizative të aviacionit civil, asetet, individët, dhe organizatat tjera për shkak të potencialit për një ngjarje të sigurisë së informacionit. Rreziqet e sigurisë së informacionit shoqërohen me potencialin që kërcënimet do të shfrytëzojnë dobësitë e një aseti të informacionit ose grupi të aseteve të informacionit;  (5) ‘kërcënim’ do të thotë një shkelje e mundshme e sigurisë së informacionit që ekziston kur ekziston një entitet, rrethanë, veprim ose ngjarje e cila mund të shkaktoj dëm;  (6) ‘cenueshmëria’ nënkupton një të metë apo dobësi të një aseti apo të një sistemi, procedurave, projektimit, zbatimit, ose e masave të sigurisë së informacion e cila mund të shfrytëzohet dhe të rezultojë me një shkelje të politikës së sigurisë së informacionit.  **Neni 4**  **Kërkesat që rrjedhin nga kërkesat e tjera të Unionit**  1. Kur një organizatë e referuar në nenin 2 është në përputhje me kërkesat e sigurisë të përcaktuara në Rregulloren Nr. 68 (ARKEP) mbi Sigurinë dhe Funksionimin e Duhur të Rrjeteve dhe/ose Shërbimeve të Komunikimeve Elektronike që janë të barazvlefshme me kërkesat e përcaktuara në këtë Rregullore, përputhshmëria me ato kërkesa të sigurisë do të konsiderohet se përbën përputhshmëri me kërkesat e përcaktuara në këtë Rregullore.  2. Kur një organizatë e referuar në nenin 2 është një operator apo një subjekt i referuar në programet kombëtare të aviacionit civil e Shteteve Anëtare të përcaktuara në përputhje me nenin 10 të Rregullores (MPB) Nr. 01/2009, kërkesat e sigurisë kibernetike që përmbahen në pikën 1.7 të Shtojcës së Rregullores (MPB) Nr. 04/2017 konsiderohen të barasvlershme me kërkesat e përcaktuara në këtë Rregullore, përveç në lidhje me pikën IS.D.OR.230 të Shtojcës së kësaj Rregulloreje me të cilën duhet të jetë në përputhshmëri.  3. Komisioni, pas konsultimit me AESA-n dhe Grupin e Bashkëpunimit të referuar në Rregulloren (ARKEP) Nr. 68 mbi Sigurinë dhe Funksionimin e Duhur të Rrjeteve dhe/ose Shërbimeve të Komunikimeve Elektronike, mund të nxjerr udhëzues për vlerësimin e barazvlefshmërisë së kërkesave të përcaktuara në këtë Rregullore dhe në Rregulloren Nr.68 (ARKEP).  **Neni 5**  **Autoriteti kompetent**  1. Autoritet përgjegjës për certifikimin dhe mbikëqyrjen e përputhshmërisë me këtë Rregullore do të jetë:  (a) në lidhje me organizata et referuara në nenin 2, pika (a), autoriteti kompetent i caktuar në përputhje me Shtojcën I (Pjesa 21) të Rregullores(AAC) Nr. 06/2015;  (b) në lidhje me organizata et referuara në nenin 2, pika (b), autoriteti kompetent i caktuar në përputhje me Shtojcën III (Pjesa-ADR.OR) të Rregullores (AAC) Nr. 17/2017.  2. Shtetet Anëtare, për qëllime të kësaj Rregulloreje, mund të caktojnë një subjekt të pavarur dhe autonom për të përmbushur rolin dhe përgjegjësitë e caktuara autoriteteve kompetente të përmendura në paragrafin 1. Në atë rast, masa koordinuese do të vendosen ndërmjet atij subjekti dhe autoritetet kompetent, siç referohet në paragrafin 1, për të siguruar mbikëqyrje efektive të të gjitha kërkesave që duhen të përmbushen nga organizata.  **Neni 6**  **Ndryshimi i Rregullores (AAC) Nr. 06/2015**  Shtojca I (Pjesa 21) e Rregullores (AAC) Nr. 06/2015 është ndryshuar si vijon:  Tabela e Përmbajtjes është i ndryshuar si vijon:  Titulli në vijim është futur pas titullit 21.A.139:  ’ 21.A.139A Sistemi i Menaxhimit të Sigurisë së Informacionit ';  Titulli në vijim është futur pas titullit 21.A.239:  ’21.A.239A Sistemi i Menaxhimit të Sigurisë së Informacionit ';  Pika në vijim 21.A.139A është futur pas pikës 21.A.139: 21.A.139A ‘21.A.139A Sistemi i Menaxhimit të Sigurisë së Informacionit  Përveç sistemit të menaxhimit të prodhimit të kërkuar nga pika 21.A.139, organizata prodhuese duhet të krijojë, zbatojë dhe mirëmbajë një sistem të menaxhimit të sigurisë së informacionit në përputhje me Rregulloren (AAC) nr. xx/2025 për të siguruar menaxhim të duhur të rreziqeve të sigurisë së informacionit të cilat mund të kenë ndikim në sigurinë e aviacionit.  Pika në vijim 21.A.239A është futur pas pikës 21.A.239:  ‘21.A.239A Sistemi i Menaxhimit të Sigurisë së Informacionit  Përveç sistemit të menaxhimit të projektimit të kërkuar nga pika 21.A.239, organizata projektuese do të krijojë, zbatojë dhe mirëmbajë një sistem të menaxhimit të sigurisë së informacionit në përputhje me Rregulloren (AAC) nr. xx/2025 për të siguruar menaxhim të duhur të rreziqeve të sigurisë së informacionit të cilat mund të kenë ndikim në sigurinë e aviacionit.'  **Neni 7**  **Ndryshimi i Rregullores (AAC) Nr. 17/2017**  Shtojca III (Pjesa-ADR.OR) e Rregullores (AAC) Nr. 17/2017 është i ndryshuar si vijon:  Pika vijuese ADR.OR.D.005A është futur pas pikës ADR.OR.D.005: ‘ADR.OR.D.005A Sistemi i Menaxhimit të Sigurisë së Informacionit  Operatori i aerodromit do të vendosë, zbatojë dhe mirëmbajë një sistem të menaxhimit të sigurisë së informacionit në përputhje me Rregulloren (AAC) nr. xx/2025 për të siguruar menaxhim të duhur të rreziqeve të sigurisë së informacionit të cilat mund të kenë ndikim në sigurinë e aviacionit.  pika ADR.OR.D.007 është zëvendësuar me pikën në vijim:  ‘ADR.OR.D.007 Menaxhimi i të dhënave aeronautike dhe informacionit aeronautik  Si pjesë sistemit të tij të menaxhimit, operatori i aerodromit do të zbatojë dhe mirëmbajë një sistem të menaxhimit të cilësisë që mbulon aktivitetet e mëposhtme:  aktivitetet e tij të të dhënave aeronautike ;  aktivitetet e tij të furnizimit të informacionit aeronautik.  Operatori i aerodromit, si pjesë e sistemit të tij të menaxhimit, duhet të krijojë një sistem të menaxhimit të sigurisë për të garantuar sigurinë e të dhënave operacionale që merr, ose prodhon, apo përndryshe përdor, në mënyrë që qasja në ato të dhëna operacionale kufizohet vetëm për ata që janë të autorizuar.  Sistemi i menaxhimit të sigurisë do të definojë elementët e mëposhtëm:  procedurat në lidhje me vlerësimin dhe zbutjen e rrezikut të sigurisë së të dhënave, monitorimin dhe përmirësimin e sigurisë, rishikimet e sigurisë dhe shpërndarjen e mësimeve;  mjetet e parapara për zbuluar shkeljet e sigurisë dhe për t’ju dhënë personelit paralajmërimet e duhura të sigurisë;  mjetet për të kontrolluar efektet e shkeljeve të sigurisë dhe për të identifikuar veprimet e rimëkëmbjes dhe procedurat për të parandaluar përsëritjen.  Operatori i aerodromit duhet të bëj verifikimin e sigurisë së personelit të tij në lidhje me sigurinë e të dhënave aeronautike.  Aspektet në lidhje me sigurinë e informacionit do të menaxhohen në përputhje me pikën ADR.OR.D.005A.';  Pika në vijim ADR.OR.F.045A është futur pas pikës ADR.OR.F.045: ‘ADR.OR.F.045A Sistemi i Menaxhimit të Sigurisë së Informacionit  Organizata përgjegjëse për ofrimin e SHMP-së do të vendosë, zbatojë dhe mirëmbajë një sistem të menaxhimit të sigurisë së informacionit në përputhje me Rregulloren (CAA) nr. xx/2025 për të siguruar menaxhim të duhur të rreziqeve të sigurisë së informacionit të cilat mund të kenë ndikim në sigurinë e aviacionit.'  **Neni 8**  **Hyrja në fuqi**  Kjo Rregullore do të hyj në forcë shtatë (7) ditë pas nënshkrimit të saj.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **Matej Krasniqi**  UD. Drejtori i Përgjithshëm | Director General of Civil Aviation Authority of the Republic of Kosovo,  Pursuant to Articles 21.2, 44, 61.2 and 67, of the Law No.03/L-051 on Civil Aviation (“Official Gazette of the Republic of Kosovo”, Year III, No. 28, 4 June 2008), amended by Law No. 08/L-063 for the amendment and completion of the laws related to the rationalization and establishment of the accountability lines of the Independent Agencies,    Taking into consideration,  International obligations of the Republic of Kosovo towards Multilateral Agreement on Establishing the European Common Aviation Area (hereinafter “ECAA Agreement”) since its provisional entry into force for Kosovo on 10 October 2006,  Regulation (CAA) No. 05/2020 on common rules in the field of civil aviation and establishing a European Union aviation safety agency and amending Regulation (CAA) No. 10/2015 and repealing Regulation (CAA) No. 11/2009, Regulation (CAA) No. 03/2009 and Regulation (CAA) No. 6/2009,  Regulation No. 17/2017 on requirements and administrative procedures related to aerodromes, as amended,  Hereby issues the following:  **Regulation (CAA) No. XX/2025**  **laying down rules for the application of Regulation (CAA) No. 05/2020 as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Regulations (CAA) No. 06/2015 and (CAA) No. 17/2017 and amending Regulations (CAA) No. 06/2015 and (CAA) No. 17/2017**  **Article 1**  **Subject matter**   1. The purpose of this Regulation is the partial transposition of the Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 and amending Commission Regulations (EU) No 748/2012 and (EU) No 139/2014, into the internal legal order of the Republic of Kosovo. 2. This Regulation sets out the requirements to be met by the organisations referred to in Article 2 in order to identify and manage information security risks with potential impact on aviation safety which could affect information and communication technology systems and data used for civil aviation purposes and to detect information security events and identify those which are considered information security incidents with potential impact on aviation safety and respond to, and recover from, those information security incidents.   **Article 2**  **Scope**  1. This Regulation applies to the following organisations:  (a) production organisations and design organisations subject to Subparts G and J of Section A of Annex I (Part 21) to Regulation (CAA) No. 06/2015, except design and production organisations that are solely involved in the design and/or production of ELA2 aircraft as defined in Article 1(2), point (j) of Regulation (CAA) No. 06/2015;  (b) aerodrome operators and apron management service providers subject to Annex III ‘Part Organisation Requirements (Part-ADR.OR)’ to Regulation (CAA) No. 17/2017.  2. This Regulation is without prejudice to information security and cybersecurity requirements laid down in point 1.7 of the Annex to Regulation (MIA) no. 04/2017 and in Regulation (ARKEP) No. 68 on the Security and Proper Functioning of Electronic Communications Networks and/or Services.  **Article 3**  **Definitions**  For the purpose of this Regulation, the following definitions shall apply:  (1) ‘information security’ means the preservation of confidentiality, integrity, authenticity and availability of network and information systems;  (2) ‘information security event’ means an identified occurrence of a system, service or network state indicating a possible breach of the information security policy or failure of information security controls, or a previously unknown situation that can be relevant for information security;  (3) ‘incident’ means any event having an adverse effect on the security of network and information systems as defined in Regulation (ARKEP) No. 68 on the Security and Proper Functioning of Electronic Communications Networks and/or Services;  (4) ‘information security risk’ means the risk to organisational civil aviation operations, assets, individuals, and other organisations due to the potential of an information security event. Information security risks are associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets;  (5) ‘threat’ means a potential violation of information security which exists when there is an entity, circumstance, action or event that could cause harm;  (6) ‘vulnerability’ means a flaw or weakness in an asset or a system, procedures, design, implementation, or information security measures that could be exploited and results in a breach or violation of the information security policy.  **Article 4**  **Requirements arising from other Union legislation**  1. Where an organisation referred to in Article 2 complies with security requirements laid down Regulation (ARKEP) No. 68 on the Security and Proper Functioning of Electronic Communications Networks and/or Services that are equivalent to the requirements laid down in this Regulation, compliance with those security requirements shall be considered to constitute compliance with the requirements laid down in this Regulation.  2. Where an organisation referred to in Article 2 is an operator or an entity referred to in the national civil aviation security programmes of Member States laid down in accordance with Article 10 of Regulation (MIA) No 01/2009, the cybersecurity requirements contained in point 1.7 of the Annex to Regulation (MIA) no. 04/2017 are considered to be equivalent to the requirements laid down in this Regulation, except as regards point IS.D.OR.230 of the Annex to this Regulation that shall be complied with.  3. The Commission, after consulting EASA and the Cooperation Group referred to in Regulation (ARKEP) No. 68 on the Security and Proper Functioning of Electronic Communications Networks and/or Services, may issue guidelines for the assessment of the equivalence of requirements laid down in this Regulation and Regulation (ARKEP) No. 68.  **Article 5**  **Competent authority**  1. The authority responsible for certifying and overseeing compliance with this Regulation shall be:  a. with regard to organisations referred to in Article 2, point (a), the competent authority designated in accordance with Annex I (Part 21) to Regulation (CAA) No. 06/2015;  b. with regard to organisations referred to in Article 2, point (b), the competent authority designated in accordance with Annex III (Part-ADR.OR) to Regulation (CAA) No. 17/2017.  3. Member States, may for the purposes of this Regulation, designate an independent and autonomous entity to fulfil the assigned role and responsibilities of the competent authorities referred to in paragraph 1. In that case, coordination measures shall be established between that entity and the competent authorities, as referred to in paragraph 1, to ensure effective oversight of all the requirements to be met by the organisation.  **Article 6**  **Amendment to Regulation (CAA) No. 06/2015**  Annex I (Part 21) to Regulation (CAA) No. 06/2015 is amended as follows:  the Table of Contents is amended as follows:  the following heading is inserted after heading 21.A.139: ‘21.A.139A Information security management system’;  the following heading is inserted after heading 21.A.239: ‘21.A.239A Information security management system’;  the following point 21.A.139A is inserted after point 21.A.139: ‘21.A.139A Information security management system  In addition to the production management system required by point 21.A.139, the production organisation shall establish, implement and maintain an information security management system in accordance with Regulation (CAA) no. xx/2025 in order to ensure the proper management of information security risks which may have an impact on aviation safety.  The following point 21.A.239A is inserted after point 21.A.239: ‘21.A.239A Information security management system  In addition to the design management system required by point 21.A.239, the design organisation shall establish, implement and maintain an information security management system in accordance with Regulation (CAA) no. xx/2025 in order to ensure the proper management of information security risks which may have an impact on aviation safety.’.  **Article 7**  **Amendment to Regulation (CAA) No. 17/2017**  Annex III (Part-ADR.OR) to Regulation (CAA) No. 17/2017 is amended as follows:  the following point ADR.OR.D.005A is inserted after point ADR.OR.D.005: ‘ADR.OR.D.005AInformation security management system  The aerodrome operator shall establish, implement and maintain an information security management system in accordance with Regulation (CAA) no. xx/2025 in order to ensure the proper management of information security risks which may have an impact on aviation safety.  point ADR.OR.D.007 is replaced by the following:  ‘ADR.OR.D.007 Management of aeronautical data and aeronautical information  As part of its management system, the aerodrome operator shall implement and maintain a quality management system covering the following activities:  its aeronautical data activities;  its aeronautical information provision activities.  As part of its management system, the aerodrome operator shall establish a security management system to ensure the security of operational data it receives, or produces, or otherwise employs, so that access to that operational data is restricted only to those authorised.  The security management system shall define the following elements:  the procedures relating to data security risk assessment and mitigation, security monitoring and improvement, security reviews and lesson dissemination;  the means designed to detect security breaches and to alert personnel with appropriate security warnings;  the means of controlling the effects of security breaches and of identifying recovery action and mitigation procedures to prevent reoccurrence.  The aerodrome operator shall ensure the security clearance of its personnel with respect to aeronautical data security.  The aspects related to information security shall be managed in accordance with point ADR.OR.D.005A.’;  the following point ADR.OR.F.045A is inserted after point ADR.OR.F.045: ‘ADR.OR.F.045AInformation security management system  The organisation responsible for the provision of AMS shall establish, implement and maintain an information security management system in accordance with Regulation (CAA) no. xx/2025 in order to ensure the proper management of information security risks which may have an impact on aviation safety.’.  **Article 8**  **Entry into force**  This Regulation shall enter into force on seven (7) days after its signature.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **Matej Krasniqi**  Acting Director General | Generalni Direktor Autoriteta Civilnog Vaduhoplovstva Republike Kosova,  U skladu sa članovima 21.2, 44, 61.2 i 67. Zakona br. 03/L-051 o civilnom vazduhoplovstvu (“Službeni glasnik Republike Kosovo”, godina III, br. 28, od 4. juna 2008. godine), izmenjen Zakonom br. 08/L-063 za izmenu i dopunu zakona u vezi sa racionalizacijom i uspostavljanjem linija odgovornosti nezavisnih agencija,  Uzimajući u obzir,  Međunarodne obaveze Republike Kosovo prema Multilateralnom sporazumu o uspostavljanju zajedničkog evropskog vazdušnog prostora (u daljem tekstu “ECAA sporazum”) od njegovog privremenog stupanja na snagu za Kosovo 10. oktobra 2006. godine,  Uredbu (ACV) Br. 05/2020 o zajedničkim pravilima u području civilnog vazduhoplovstva i osnivanju agencije Evropske Unije za bezbednost vazdušnog saobraćaja i izmeni Uredbi (ACV) Br. 10/2015, i stavljanju van snage Uredbe (ACV) Br. 11/2009, Uredbe (ACV) Br. 03/2009 i Uredbe (ACV) Br. 6/2009,  Uredbu (ACV) Br. 17/2017 o uslovima i upravnim postupcima vezanih za aerodrome, izmenjen,  Izdaje sledeću:  **Uredbu (ACV) br. XX/2025**  **o utvrđivanju pravila za primenu Uredbe (ACV) br. 05/2020 u pogledu zahteva za upravljanje rizicima informacione bezbednosti koji mogu imati uticaj na bezbednost vazdušnog saobraćaja za organizacije obuhvaćene Uredbama (ACV) br. 06/2015 i (ACV) br. 17/2017, kao i o izmenama i dopunama Uredbi (ACV) br. 06/2015 i (ACV) br. 17/2017**  **Član 1**  **Predmet uredbe**   1. Svrha ove Uredbe je sprovođenje Delegirane Uredbe Evropske Unije (EU) 2022/1645 od 14. jula 2022. godine kojim se utvrđuju pravila za primenu Uredbe (EU) 2018/1139 Evropskog parlamenta i Saveta, u vezi sa zahtevima za upravljanje rizicima po bezbednost informacija sa potencijalnim uticajem na bezbednost vazduhoplovstva za organizacije obuhvaćene Uredbama Komisije (EU) br. 748/2012 i (EU) br. 139/2014 i kojim se menjaju Uredbe Komisije (EU) br. 748/2012 i (EU) br. 139/2014, u unutrašnji pravni poredak Republike Kosovo. 2. Ova uredba utvrđuje zahteve, koje moraju da ispune organizacije navedene u članu 2 kako bi identifikovale i upravljale rizicima u vezi sa informacionom bezbednošću, sa potencijalnim uticajem na bezbednost vazduhoplovstva koji bi mogli uticati na sisteme informacione i komunikacione tehnologije i podatke koji se koriste u svrhe civilnog vazduhoplovstva, kao i da bi otkrile događaje u vezi sa informacionom bezbednošću i identifikovale one koji se smatraju incidentima u vezi sa informacionom bezbednošću sa potencijalnim uticajem na bezbednost vazduhoplovstva, kao i da bi reagovale na te incidente u vezi sa informacionom bezbednošću i oporavile se od istih.   **Član 2**  **Delokrug**  1. Ova uredba se primenjuje na sledeće organizacije:  (a) proizvodne organizacije i projektantske organizacije koje podležu pod-delovima G i J Odeljka A Aneksa I (Deo 21) Uredbe (ACV) br. 06/2015, osim organizacija za projektovanje i proizvodnju koje su isključivo uključene u projektovanje i/ili proizvodnju aviona ELA2 kako je definisano u članu 1(2), tačka (j) Uredbe (ACV) br. 06/2015;  (b) Operatori aerodroma i pružaoci usluga upravljanja platformom koji podležu Aneksu III „Zahtevi za deo organizacije (Deo ADR.OR)“ Uredbe (ACV) br. 17/2017.  2. Ova uredba ne utiče na zahteve za informacionu bezbednost i sajber bezbednost utvrđenih u tački 1.7 Aneksa Uredbe (MUP) br. 04/2017 i u Uredbi (RAEPK) br. 68 o bezbednosti i pravilnom funkcionisanju elektronskih komunikacionih mreža i/ili usluga.  **Član 3**  **Definicije**  Za potrebe ove Uredbe, primenjuju se sledeće definicije:  (1) „bezbednost informacija“ znači očuvanje poverljivosti, integriteta, autentičnosti i dostupnosti mreže i informacionih sistema;  (2) „incident informacione bezbednosti“ znači identifikovanu pojavu stanja sistema, usluge ili mreže koja ukazuje na moguće kršenje politike bezbednosti informacija ili neuspeh kontrola bezbednosti informacija, ili prethodno nepoznatu situaciju koja može biti relevantna za bezbednost informacija;  (3) „incident“ znači svaki događaj koji ima negativan uticaj na bezbednost mreže i informacionih sistema kako je definisano u Uredbi (RAEPK) br. 68 o bezbednosti i pravilnom funkcionisanju elektronskih komunikacionih mreža i/ili usluga;  (4) „rizik po bezbednost informacija“ znači rizik za organizacione operacije civilnog vazduhoplovstva, sredstva, pojedince i druge organizacije zbog mogućih dešavanja u vezi sa bezbednošću informacija. Rizici po bezbednost informacija povezani su sa mogućnošću da pretnje iskoriste ranjivosti informacione imovine ili grupe informacionih imovine;  (5) „pretnja“ znači potencijalno kršenje bezbednosti informacija koje postoji kada postoji entitet, okolnost, radnja ili događaj koji bi mogao prouzrokovati štetu;  (6) „ranjivost“ znači mana ili slabost u imovini ili sistemu, procedurama, dizajnu, implementaciji ili merama bezbednosti informacija koja bi mogla biti iskorišćena i rezultira kršenjem ili povredom politike bezbednosti informacija.  **Član 4**  **Zahtevi koji proizilaze iz drugog zakonodavstva Unije**  1. Kada organizacija na koju se odnosi član 2. ispunjava bezbednosne zahteve utvrđene Uredbom (RAEPK) br. 68 o bezbednosti i pravilnom funkcionisanju elektronskih komunikacionih mreža i/ili usluga koji su ekvivalentni zahtevima utvrđenim ovom uredbom, usklađenost sa tim bezbednosnim zahtevima smatraće se usklađenošću sa zahtevima utvrđenim ovom uredbom.  2. Kada je organizacija navedena u članu 2 operater ili subjekt naveden u nacionalnom sistemu civilnog vazduhoplovstva bezbednosnih programa država članica utvrđenih u skladu sa članom 10. Uredbe (MUP) br. 01/2009, zahtevi za sajber bezbednost sadržani u tački 1.7 Aneksa Uredbe (MUP) br. 04/2017 smatraju se ekvivalentnim zahtevima utvrđenim ovom uredbom, osim u pogledu tačke IS.D.OR.230 Aneksa ove uredbe koja se mora poštovati.  3. Komisija, nakon konsultacija sa EASA i Grupom za saradnju na koju se odnosi Uredba (RAEPK) br. 68 o bezbednosti i pravilnom funkcionisanju elektronskih komunikacionih mreža i/ili usluga, može izdati smernice za procenu ekvivalencije zahteva utvrđenih ovom uredbom i Uredbom (RAEPK) br. 68.  **Član 5**  **Nadležni organ**  1. Organ odgovoran za sertifikaciju i nadzor usklađenosti sa ovom uredbom je:  (a) u vezi sa organizacijama navedenim u članu 2, tačka (a), nadležni organ određen u skladu sa Aneksom I (Deo 21) Uredbe (ACV) br. 06/2015;  (b) u vezi sa organizacijama navedenim u članu 2, tačka (b), nadležni organ određen u skladu sa Aneksom III (Deo-ADR.OR) Uredbe (ACV) br. 17/2017.  2. Države članice mogu, u svrhu ove uredbe, odrediti nezavisan i autonoman entitet koji će ispunjavati dodeljenu ulogu i odgovornosti nadležnih organa iz stava 1. U tom slučaju, uspostavljaju se mere koordinacije između tog entiteta i nadležnih organa, kako je navedeno u stavu 1, kako bi se obezbedio efikasan nadzor nad svim zahtevima koje organizacija treba da ispuni.  **Član 6**  **Izmene i dopune Uredbe (ACV) br. 06/2015**  Aneks I (Deo 21) Uredbe (ACV) br. 06/2015 se menja kao što sledi:  (1) tabela sadržaja se menja kao što sledi:  (a) Sledeći naslov se ubacuje posle naslova 21.A.139: '21.A.139A Sistem upravljanja bezbednošću informacija';  (b) Sledeći naslov se ubacuje posle naslova 21.A.239: '21.A.239A Sistem upravljanja bezbednošću informacija';  (2) nakon tačke 21.A.139 umeće se sledeća tačka 21.A.139A:  '21.A.139A Sistem upravljanja bezbednošću informacija  Pored sistema upravljanja proizvodnjom, koji zahteva tačka 21.A.139, proizvodna organizacija mora da uspostavi, implementira i održava sistem upravljanja bezbednošću informacija u skladu sa Uredbom (ACV) br. xx/2025 kako bi se osiguralo pravilno upravljanje rizicima bezbednosti informacija a koji mogu imati uticaj na bezbednost vazduhoplovstva.  Nakon tačke 21.A.239 umeće se sledeća tačka 21.A.239A: '21.A.239A Sistem upravljanja bezbednošću informacija  Pored sistema upravljanja projektovanjem koji zahteva tačka 21.A.239, organizacija za projektovanje mora da uspostavi, implementira i održava sistem upravljanja bezbednošću informacija u skladu sa Uredbom (ACV) br. xx/2025 kako bi se obezbedilo pravilno upravljanje rizicima po bezbednost informacija, koji mogu imati uticaj na bezbednost vazduhoplovstva.“  **Član 7**  **Izmene i dopune Uredbe (ACV) br. 17/2017**  Aneks III (Deo-ADR.AR) Uredbe (ACV) br. 17/2017 menja se kao što sledi:  (1) nakon tačke ADR.OR.D.005 umeće se sledeća tačka ADR.OR.D.005A: ADR.OR.D.005A Sistem upravljanja bezbednošću informacija  Operator aerodroma uspostavlja, implementira i održava sistem upravljanja bezbednošću informacija u skladu sa Uredbom (ACV) br. xx/2025 kako bi se osiguralo pravilno upravljanje rizicima bezbednosti informacija, koji mogu imati uticaj na bezbednost vazduhoplovstva.  (2) tačka ADR.OR.D.007 zamenjuje se sledećom:  'ADR.OR.D.007 Upravljanje vazduhoplovnim podacima i vazduhoplovnim informacijama  (a) Kao deo svog sistema upravljanja, operater aerodroma mora da implementira i održava sistem upravljanja kvalitetom koji obuhvata sledeće aktivnosti:  (1) svoje aktivnosti u vezi sa vazduhoplovnim podacima;  (2) svoje aktivnosti pružanja vazduhoplovnih informacija.  (b) Kao deo svog sistema upravljanja, operater aerodroma uspostavlja sistem upravljanja bezbednošću kako bi se osigurala bezbednost operativnih podataka koje prima, proizvodi ili na drugi način koristi, tako da pristup tim operativnim podacima bude ograničen samo na one koji su ovlašćeni.  (c) Sistem upravljanja bezbednošću mora definisati sledeće elemente:  (1) procedure koje se odnose na procenu i ublažavanje rizika bezbednosti podataka, praćenje i unapređenje bezbednosti, preglede bezbednosti i širenje lekcija;  (2) namenjena sredstva za otkrivanje bezbednosnih propusta i upozoravanje osoblja odgovarajućim bezbednosnim upozorenjima;  (3) sredstva za kontrolu efekata kršenja bezbednosti i za identifikovanje mera oporavka i postupaka za ublažavanje kako bi se sprečilo ponavljanje.  (d) Operator aerodroma je dužan da obezbedi bezbednosnu proveru svog osoblja u pogledu bezbednosti vazduhoplovnih podataka.  (e) Aspekti vezani za bezbednost informacija upravljaju se u skladu sa tačkom ADR.OR.D.005A.“;  (3) posle tačke ADR.OR.F.045 umeće se sledeća tačka ADR.OR.F.045A:  ADR.OR.F.045A Sistem upravljanja bezbednošću informacija  Organizacija odgovorna za obezbeđivanje AMS-a mora da uspostavi, implementira i održava sistem upravljanja bezbednošću informacija u skladu sa Uredbom (ACV) br. xx/2025, kako bi se obezbedilo pravilno upravljanje rizicima po bezbednost informacija a koji mogu imati uticaj na bezbednost vazduhoplovstva.“  **Član 8**  **Stupanje na snagu**  Ova Uredba stupa na snagu sedam (7) dana od dana potpisivanja.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **Matej Krasniqi**  Sd. Generalni direktor |

*SHTOJCË*

**SIGURIA E INFORMACIONIT – KËRKESAT OGANIZATIVE**

**[PJESA- IS.D.OR]**

IS.D.OR.100 Fushëveprimi

IS.D.OR.200 Sistemi i menaxhimit të sigurisë së informacionit

IS.D.OR.205 Vlerësimi i rrezikut të sigurisë së informacionit IS.D.OR.210

Trajtimi i rrezikut të sigurisë së informacionit IS.D.OR.215 Skema e raportimit të

brendshëm të rrezikut të sigurisë së informacionit

IS.D.OR.220 Incidentet e sigurisë së informacionit - zbulimi, reagimi dhe rimëkëmbja

IS.D.OR.225 Përgjigja ndaj gjetjeve për të cilat është bërë njoftimi nga ana e autoritetit kompetent

IS.D.OR.230 Skema e raportimit ë jashtëm të rrezikut të sigurisë së informacionit

IS.D.OR.235 Kontraktimi i aktiviteteve për menaxhimin e sigurisë së informacionit

IS.D.OR.240 Kërkesat për Personelin

IS.D.OR.245 Mbajtja e shënimeve/të dhënave

IS.D.OR.250 Manuali për menaxhimin e sigurisë së informacionit (MMSI) IS.D.OR.255

Ndryshimet e sistemit të menaxhimit të sigurisë së informacionit IS.D.OR.260

Përmirësimi i vazhdueshëm

**IS.D.OR.100 Fushëveprimi**

Kjo Pjesë vendos kërkesat që duhen të përmbushen nga organizatat e referuara në nenin 2 të kësaj Rregulloreje.

**IS.D.OR.200 Sistemi i Menaxhimit të Sigurisë së Informacionit (SMSI)**

1. Për të arritur objektivat e përcaktuara në nenin 1, organizata duhet të krijojë, zbatojë dhe mirëmbajë një sistem të menaxhimit të sigurisë së informacionit (SMSI) i cili siguron që organizata:
   1. themelon një politikë për sigurinë e informacionit që përcakton parimet e përgjithshme të organizatës në lidhje me ndikimin e mundshëm të rreziqeve të sigurisë së informacionit në sigurinë e aviacionit;
   2. identifikon dhe rishikon rreziqet e sigurisë së informacionit në përputhje me pikë IS.D.OR.205;
   3. definon dhe zbaton masa të trajtimit të rrezikut të sigurisë së informacionit në përputhje me pikën IS.D.OR.210;
   4. zbaton një skemë raportuese të brendshme të sigurisë së informacionit në përputhje me pikën IS.D.OR.215;
   5. definon dhe zbaton, në përputhje me pikën IS.D.OR.220, masat e nevojshme për zbulimin e ngjarjeve të sigurisë së informacionit, identifikon ato ngjarje që konsiderohen si incidente me një ndikim të mundshëm në sigurinë e aviacionit përveç siç lejohet nga pika IS.D.OR.205(e), dhe u përgjigjet dhe rimëkëmbet nga ato incidente të sigurisë së informacionit;
   6. zbaton masat për të cilat është njoftuar nga autoriteti kompetent si reagim i menjëhershëm ndaj një incidenti ose cenueshmërie të sigurisë së informacionit me ndikim në sigurinë e aviacionit;
   7. merr masat e duhura, në përputhje me pikën IS.D.OR.225, për të adresuar gjetjet e njoftuara nga autoriteti kompetent;
   8. zbaton një skemë raportuese të jashtme në përputhje me pikën IS.D.OR.230 në mënyrë që t'i mundësojë autoritetit kompetent të ndërmarrë veprimet e duhura;
   9. vepron në përputhje me kërkesat e përfshira në pikën IS.D.OR.235 kur e kontrakton ndonjë pjesë të aktiviteteve të referuara në pikën IS.D.OR.200 me organizatat e tjera;
   10. vepron në përputhje me kërkesat e përcaktuara në pikën IS.D.OR.240;
   11. vepron në përputhje me kërkesat për mbajtje të shënimeve/të dhënave të përcaktuara në pikën IS.D.OR.245;
   12. monitoron përputhshmërinë e organizatës me kërkesat e kësaj Rregulloreje dhe i ofron komente mbi gjetjet menaxherit përgjegjës ose, në rastin e organizatave projektuese, drejtuesit të organizatës projektuese, në mënyrë që të sigurojë zbatim efektiv të veprimeve korrigjuese;
   13. mbron, pa paragjykuar kërkesat përkatëse mbi raportimin e incidenteve, konfidencialitetin e çfarëdo informacioni të cilin organizata ka mundësi ta ketë pranuar nga një organizatë tjetër , sipas nivelit të ndjeshmërisë së informacionit.
2. Për të përmbushur kërkesat e referuara në Nenin 1 në mënyrë të vazhdueshme, organizata do të zbatojë një proces të vazhdueshëm përmirësimi në përputhje me pikën IS.D.OR.260.
3. Organizata do të dokumentojë, në përputhje me pikën IS.D.OR.250, të gjitha proceset, procedurat, rolet dhe përgjegjësitë kyçe të kërkuara për të përmbushur pikën IS.D.OR.200(a) dhe të krijojë një proces për ndryshimin e këtij dokumentimi. Ndryshimet në këto procese, procedura, role dhe përgjegjësi duhet të menaxhohen në përputhje me pikën IS.D.OR.255.
4. Proceset, procedurat, rolet dhe përgjegjësitë e vendosura nga organizata në mënyrë që të jetë në përputhje me pikën IS.D. OR.200(a) do të korrespondojë me natyrën dhe kompleksitetin e aktiviteteve të saj, bazuar në një vlerësim të rreziqeve të sigurisë së informacionit të qenësishme për ato aktivitete, dhe mund të integrohet brenda sistemeve të tjera ekzistuese të menaxhimit tashmë të zbatuara nga organizata.
5. Pa paragjykuar detyrimin për të përmbushur kërkesat e raportimit që janë përfshirë në Rregulloren (AAC) nr. 09/2017 për raportimin, analizën dhe përcjelljen e dukurive në aviacionin civil dhe kërkesat e pikës IS.D.OR.200 (a) (13), organizatës mund t'i jepet miratimi nga autoriteti kompetent për të mos zbatuar kërkesat e përmendura në pikat (a) deri (d)) dhe kërkesat e ndërlidhura të përfshira në pikat nga IS.D.OR.205 deri tek IS.D.OR.260, nëse ajo demonstron në mënyrë që përmbush kërkesat e atij autoriteti se aktivitetet, objektet dhe burimet e saj, si dhe shërbimet me të cilat operon, i ofron, i merr dhe i mirëmban, nuk paraqesin asnjë rrezik për sigurinë e informacionit me ndikim të mundshëm në sigurinë e aviacionit as për veten dhe as për organizatat e tjera. Miratimi do të bazohet në një vlerësim të dokumentuar të rrezikut të sigurisë së informacionit të kryer nga organizata apo nga një palë e tretë në përputhje me pikën IS.D.OR.205 dhe të rishikohet dhe miratohet nga autoriteti i saj kompetent.

Vlefshmëria e vazhdueshme e atij miratimi do të rishikohet nga ana e autoritetit kompetent pas ciklit të zbatueshëm të mbikëqyrjes dhe sa herë që zbatohen ndryshime në fushëveprimin e punës së organizatës.

**IS.D.OR.205 Vlerësimi i rrezikut të sigurisë së informacionit**

1. Organizata do të identifikojë të gjithë elementët e saj, të cilët mund të ekspozohen ndaj rreziqeve të sigurisë së informacionit. Kjo do të përfshijë:
   1. aktivitetet, objektet dhe mjediset dhe burimet e organizatës, si dhe shërbimet me të cilat organizata operon, i ofron, i merr, apo i mirëmban;
   2. pajisjet, sistemet, të dhënat dhe informacionet të cilat kontribuojnë në funksionimin e elementëve të renditur në pikën (1).
2. Organizata do të identifikojë ndërfaqet që i ka me organizatat e tjera, të cilat mund të rezultojnë në ekspozimin e ndërsjellë ndaj rreziqeve të sigurisë së informacionit.
3. Në lidhje me elementë dhe ndërfaqet e referuara në pikën (a) dhe (b), organizata do të identifikojë rreziqet e sigurisë së informacionit që mund të kenë një ndikim të mundshëm në sigurinë e aviacionit. Për çdo rrezik të identifikuar, organizata do të:
   1. caktojë një nivel rreziku sipas një klasifikimi të paracaktuar të vendosur nga organizata;

* 1. ndërlidh çfarëdo rreziku dhe nivelin e tij me elementin përkatës ose ndërfaqen e identifikuar në përputhje me pikat (a) dhe (b).

Klasifikimi i paracaktuar i referuar në pikën (1) do të marrë në konsideratë potencialin e paraqitjes së skenarit të kërcënimit dhe ashpërsinë e pasojave të tij të sigurisë. Bazuar në atë klasifikim dhe duke marrë parasysh nëse organizata ka një proces të strukturuar dhe të përsëritshëm të menaxhimit të rrezikut për operacionet, organizata duhet të jetë në gjendje të përcaktojë nëse rreziku është i pranueshëm apo duhet të trajtohet në përputhje me pikën IS.D.OR.210.

Për të lehtësuar krahasueshmërinë e ndërsjellë të vlerësimeve të rreziqeve, caktimi i nivelit të rrezikut në përputhje me pikën

1. do të marr parasysh informacionet relevante të siguruara në koordinim me organizatat e referuara në pikën (b).
2. Organizata do ta rishikojë dhe përditësojë vlerësimin e rrezikut të kryer në përputhje me pikat (a), (b) dhe (c) në cilëndo nga situatat në vijim, kur:
   1. ka një ndryshim të elementëve që i nënshtrohen rreziqeve të sigurisë së informacionit;
   2. ka një ndryshim në ndërfaqet ndërmjet organizatës dhe organizatave të tjera, ose në rreziqet e komunikuara nga organizatat e tjera;
   3. ka një ndryshim në informacionet ose njohuritë e përdorura për identifikimin, analizën dhe klasifikimin e rreziqeve;
   4. ka mësime që janë nxjerrë nga analiza e incidenteve të sigurisë së informacionit.

**IS.D.OR.210 Trajtimi i rrezikut të sigurisë së informacionit**

1. Organizata do të zhvillojë masa për të adresuar rreziqet e papranueshme të identifikuara në përputhje me pikën IS.D. OR.205, t'i zbatojë ato në kohën e duhur dhe të kontrollojë efektivitetin e tyre të vazhdueshëm. Këto masa do t'i mundësojnë organizatës që të:
   1. kontrollojë rrethanat që kontribuojnë në ndodhjen efektive të skenarit të kërcënimit;
   2. zvogëlojë pasojat për sigurinë e aviacionit që ndërlidhet me materializimin e skenarit të kërcënimit;
   3. shmang rreziqet.

Ato masa nuk do të prezantojnë ndonjë rrezik të ri të mundshëm të papranueshëm për sigurinë e aviacionit.

1. Personi i referuar në pikën IS.D.OR.240 (a) dhe (b) dhe personeli tjetër i prekur i organizatës do të informohen për rezultatin e vlerësimit të rrezikut të kryer në përputhje me pikën IS.D.OR.205, skenarët përkatës të kërcënimit dhe masat që do të zbatohen.

Organizata gjithashtu do t’i informojë organizatat me të cilat ka një ndërfaqe në përputhje me pikën IS.D.OR.205

(b) për çfarëdo rreziku të përbashkët ndërmjet të dyja organizatave.

**IS.D.OR.215 Skema e raportimit të brendshëm të sigurisë së informacionit**

1. Organizata do të krijojë një skemë të raportimit të brendshëm për të mundësuar mbledhjen dhe vlerësimin e ngjarjeve të sigurisë së informacionit, përfshirë ato që duhet të raportohen në përputhje me pikën IS.D.OR.230.
2. Kjo skemë dhe procesi i referuar në pikën IS.D.OR.220 do t’i mundësoj organizatës që të:
   1. identifikojë se cilat nga ngjarjet e raportuara në përputhje me pikën (a) konsiderohen incidente ose cenueshmëri të sigurisë së informacionit me ndikim të mundshëm në sigurinë e aviacionit;
   2. identifikojë shkaqet dhe faktorët që kontribuojnë në, incidentet dhe cenueshmëritë e sigurisë së informacionit të identifikuara në përputhje me pikën (1), dhe t’ adresojë ato si pjesë e procesit të menaxhimit të rrezikut të sigurisë së informacionit në përputhje me pikat IS.D.OR.205 dhe IS.D.OR.220;
   3. sigurojë një vlerësim të të gjithë informacionit përkatës të njohur në lidhje me incidentet dhe cenueshmëritë e sigurisë së informacionit të identifikuara në përputhje me pikën (1);
   4. sigurojë zbatimin e një metode për shpërndarjen e brendshme të informacionit siç është e nevojshme.
3. Nga çdo organizate e kontraktuar e cila mund ta ekspozojë organizatën ndaj rreziqeve të sigurisë së informacionit me një ndikim të mundshëm në sigurinë e aviacionit do të kërkohet t’ia raportojë ngjarjet e sigurisë së informacionit organizatës. Ato raporte do të dorëzohen duke përdorur procedurat e përcaktuara në marrëveshjet specifike kontraktuale dhe do të vlerësohen në përputhje me pikën (b).
4. Organizata do të bashkëpunojë në hetime me çfarëdo organizatë tjetër që ka një kontribut të rëndësishëm në sigurinë e informacionit në aktivitetet e saja vetanake.
5. Organizata mund ta integroj atë skemë të raportimit me skema të tjera të raportimit të cilat tashmë i ka zbatuar.

**IS.D.OR.220 Incidentet e sigurisë së informacionit – zbulimi, reagimi dhe rimëkëmbja**

1. Bazuar në rezultatin e vlerësimit të rrezikut të kryer në përputhje me pikën IS.D.OR.205 dhe rezultatin e trajtimit të rrezikut të kryer në përputhje me pikën IS.D.OR.210, organizata do të zbatojë masa për zbulimin e incidenteve dhe cenueshmërive që tregojnë materializimin e mundshëm të rreziqeve të papranueshme dhe që mund të kenë një ndikim të mundshëm në sigurinë e aviacionit. Këto masa zbulimi do t'i mundësojnë organizatës që të:
   1. identifikojë devijimet nga kriteret e paracaktuara bazë të performancës funksionale;
   2. jep paralajmërime për aktivizimin e masave të duhura reaguese, në rast të çfarëdo devijimi.
2. Organizata do të zbatojë masa për t'iu përgjigjur çfarëdo kushteve të ngjarjes së identifikuar në përputhje me pikën (a) e cila mund të zhvillohet ose të shndërrohet në një incident të sigurisë së informacionit. Këto masa reaguese do t'i mundësojnë organizatës që të:
   1. nis reagimin ndaj paralajmërimeve të përmendura në pikën (a) (2) duke aktivizuar burimet dhe rrjedhën e paracaktuar të veprimeve;
   2. kufizojë përhapjen e një sulmi dhe shmangien e materializimit të plotë të një skenari të kërcënimit;
   3. kontrollojë mënyrën e dështimit të elementëve të prekur të definuar në pikën IS.D.OR.205(a).
3. Organizata do të zbatojë masa të cilat synojnë rimëkëmbjen nga incidentet e sigurisë së informacionit, duke përfshirë masat emergjente, nëse është e nevojshme. Këto masa të rimëkëmbjes do t'i mundësojnë organizatës që të:
   1. eliminojë gjendjen e cila shkaktoi incidentin, ose ta kufizojë atë në një nivel të tolerueshëm;
   2. të arrij një gjendje të sigurt të elementëve të prekur të definuar në pikën IS.D.OR.205(a) brenda një afati për rimëkëmbje të definuar paraprakisht nga organizata.

**IS.D.OR.225 Përgjigja ndaj gjetjeve për të cilat është bërë njoftimi nga ana e autoritetit kompetent**

1. Pas marrjes së njoftimit mbi gjetjet të parashtruar nga autoriteti kompetent, organizata do të:
   1. identifikojë shkakun rrënjësor ose shkaqet dhe faktorët që kontribuojnë në mospërputhje;
   2. definojë një plan të veprimeve korrigjuese;
   3. demonstrojë korrigjimin e mos-përputhshmërisë që përmbushë kërkesat e autoritetit kompetent.
2. Veprimet e referuara në pikën (a) do të kryhen brenda periudhës së rënë dakord me autoritetin kompetent.

**IS.D.OR.230 Skema e raportimit të jashtëm të sigurisë së informacionit**

1. Organizata do të zbatojë një sistem raportimi të sigurisë së informacionit i cili përputhet me kërkesat e përcaktuara në Rregulloren (AAC) nr. 09/2017 dhe ndryshimet e tij, nëse zbatohen për organizatën.
2. Pa paragjykuar detyrimet e Rregullores (AAC) nr. 09/2017, organizata do të sigurojë që çdo incident apo cenueshmëri e sigurisë së informacionit, që mund të përfaqësojë një rrezik domethënës për sigurinë e aviacionit, t'i raportohet autoritetit të saj kompetent. Për më tepër:
   1. kur një incident ose cenueshmëri e tillë prek mjetin ajror apo sistemin ose komponentin e ndërlidhur, organizata do t’i raportojë për të edhe mbajtësit të miratimit të dizajnit;
   2. kur një incident ose cenueshmëri e tillë prek një sistem ose element përbërës të përdorur nga organizata, organizata do t'ia raportojë atë organizatës përgjegjëse për dizajnin e sistemit ose elementit përbërës.
3. Organizata do të raportojë mbi kushtet e referuara në pikën (b) siç vijon:
   1. një njoftim do t'i dorëzohet autoritetit kompetent dhe, nëse është e aplikueshme, mbajtësit të miratimit të dizajnit ose organizatës përgjegjëse për dizajnin e sistemit ose elementit përbërësit, sapo që organizata të jetë e njohur me gjendjen;
   2. një raport do t'i dorëzohet autoritetit kompetent dhe, nëse është e aplikueshme, mbajtësit të miratimit të dizajnit ose organizatës përgjegjëse për dizajnin e sistemit ose elementit përbërës, sa më shpejt të jetë e mundur, por jo më shumë se 72 orë nga koha kur organizata është e njohur me gjendjen, përveç rasteve kur rrethana të jashtëzakonshme e pengojnë këtë.

Raporti duhet të përgatitet në formën e përcaktuar nga autoriteti kompetent dhe duhet t’i përmbajë të gjitha informacionet relevante rreth gjendjes e cila është e njohur për organizatën;

* 1. një raport pasues mbi gjendjen do t'i dorëzohet autoritetit kompetent dhe, nëse është e aplikueshme, mbajtësit të miratimit të dizajnit ose organizatës përgjegjëse për dizajnin e sistemit ose elementit përbërës, ku ofrohen hollësi të veprimeve të cilat organizata i ka ndërmarrë ose synon t’i ndërmarrë për t’u rimëkëmbur nga incidenti dhe veprimet që synon t’i ndërmerr për të parandaluar incidente të ngjashme të sigurisë së informacionit në të ardhmen.

Raporti pasues do të dorëzohet sapo të jenë identifikuar këto veprime dhe do të përgatitet në formën e përcaktuar nga autoriteti kompetent.

**IS.D.OR.235 Kontraktimi i aktiviteteve për menaxhimin e sigurisë së informacionit**

1. Organizata do të sigurojë që, kur kontrakton ndonjë pjesë të aktiviteteve të referuara në pikën IS.D.OR.200 me organizata të tjera, aktivitetet e kontraktuara të jenë në përputhje me kërkesat e kësaj Rregulloreje dhe organizata e kontraktuar të punojë nën mbikëqyrjen e saj. Organizata do të sigurojë që rreziqet të cilat lidhen me aktivitetet e kontraktuara menaxhohen në mënyrë të përshtatshme.
2. Organizata do të sigurojë që autoriteti kompetent të ketë qasje pas kërkesës që i ka bërë organizatës së kontraktuar për të përcaktuar përputhshmërinë e vazhdueshme me kërkesat e aplikueshme të përcaktuara në këtë Rregullore.

**IS.D.OR.240 Kërkesat për personelin**

1. Menaxheri përgjegjës i organizatës ose, në rastin e organizatave të projektimit, drejtuesi i organizatës së projektimit, i caktuar në përputhje me Rregullorja (AAC) Nr. 06/2015 dhe Rregulloren (AAC) Nr. 17/2017 siç referohet në pikat 1(a) dhe (b) të nenit 2 të kësaj Rregulloreje, do të ketë autoritetin e korporatës për të siguruar që të gjitha aktivitetet e kërkuara nga kjo Rregullore mund të financohen dhe kryhen. Ai person do të:
   1. sigurojë që të gjithë burimet e nevojshme janë të disponueshme për të qenë në përputhshmëri me kërkesat e kësaj Rregulloreje;
   2. themelojë dhe promovojë politikën e sigurisë së informacionit të referuar në pikën IS.D.OR.200(a)(1);
   3. demonstrojë një kuptueshmëri bazike të kësaj Rregulloreje.
2. Menaxheri përgjegjës ose, në rastin e organizatave projektuese, drejtuesi i organizatës së projektimit, do të caktojë një person ose grup personash për të siguruar që organizata vepron në përputhje me kërkesat e kësaj Rregulloreje dhe do të definojë shtrirjen e autoritetit të tyre. Ai person apo grup personash do t'i raportojë drejtpërdrejt menaxherit përgjegjës ose, në rastin e organizatave të projektimit, drejtuesit të organizatës projektuese dhe do të posedojë/në njohuritë, sfondin dhe përvojën e duhur për të përmbushur përgjegjësitë e tij/tyre. Në procedurë do të përcaktohet se kush e zëvendëson një person të caktuar në rast të mungesës së zgjatur të atij personi.
3. Menaxheri përgjegjës ose, në rastin e organizatave projektuese, drejtuesi i organizatës së projektimit do të emërojë një person ose grup personash me përgjegjësi për të menaxhuar funksionin e monitorimit të përputhshmërisë të referuar në pikën IS.D.OR.200(a)(12).
4. Kur organizata ndan strukturat organizative të sigurisë së informacionit, politikat, proceset dhe procedurat, me organizata të tjera ose me fusha të organizatës së tyre që nuk janë pjesë e miratimit ose deklaratës, menaxheri përgjegjës ose, në rastin e organizatave projektuese, drejtuesi i organizatës projektuese, mund t'ia delegojë aktivitetet e tij një personi përgjegjës të përbashkët.

Në një rast të tillë, masa të koordinimit do të vendosen ndërmjet menaxherit përgjegjës të organizatës ose, në rastin e organizatave projektuese, drejtuesit të organizatës projektuese dhe personit përgjegjës të përbashkët për të siguruar integrimin e duhur të menaxhimit të sigurisë së informacionit brenda organizatës.

1. Menaxheri përgjegjës ose drejtuesi i organizatës projektuese, apo personi përgjegjës i përbashkët i referuar në pikën (d), do të ketë autoritetin e korporatës për të themeluar dhe mirëmbajtur strukturat organizative, politikat, proceset dhe procedurat e nevojshme për zbatimin e pikës IS.D.OR.200.
2. Organizata do të ketë të vendosur një proces që të sigurojë se ata kanë personel të mjaftueshëm në detyrë për të kryer aktivitetet e mbuluara nga kjo Shtojcë.
3. Organizata do të ketë të vendosur një proces që të sigurojë se personeli i referuar në pikën (f) e posedon zotësinë e nevojshme për të kryer detyrat e tyre.
4. Organizata do të ketë një proces të vendosur për të siguruar që personeli i pranon përgjegjësitë që ndërlidhen me rolet dhe detyrat që u janë caktuar atyre.
5. Organizata do të sigurojë që identiteti dhe besueshmëria e personelit që ka qasje në sistemet e informacionit dhe të dhënat që i nënshtrohen kërkesave të kësaj rregulloreje janë përcaktuar siç duhet.

**IS.D.OR.245 Mbajtja e shënimeve/të dhënave**

1. Organizata do të mbajë shënime për aktivitetet e saj të menaxhimit të sigurisë së informacionit
   1. Organizata do të sigurojë që të dhënat e mëposhtme janë të arkivuara dhe të gjurmueshme:
      1. çfarëdo miratimi i marrë dhe çfarëdo vlerësimi shoqërues i rrezikut të sigurisë së informacionit në përputhje me pikën IS.D. OR. 200(e);
      2. kontratat për aktivitetet e referuara në pikën IS.D.OR.200(a)(9);
      3. të dhënat për proceset kyçe të referuara në pikën IS.D.OR.200(d);
      4. të dhënat e rreziqeve të identifikuara në vlerësimin e rrezikut të referuar në pikën IS.D.OR.205 së bashku me masat e trajtimit të rrezikut të ndërlidhur të referuara në pikën IS.D.OR.210;
      5. të dhënat e informacioneve të incidenteve të sigurisë dhe cenueshmërive të raportuara në përputhje skemat e raportimit të referuara në pikat IS.D.OR.215 dhe IS.D.OR.230;
      6. të dhënat e atyre informacioneve të ngjarjeve të sigurisë për të cilat mund të ketë nevojë që të rivlerësohen për të zbuluar incidentet e pazbuluara të sigurisë ose cenueshmërisë së informacionit.
   2. Të dhënat e referuara në pikën (1)(i) do të ruhen të paktën deri 5 vite pasi që miratimi të ketë humbur vlefshmërinë e tij.
   3. Të dhënat e referuara në pikën (1)(ii) duhet të ruhen të paktën deri në 5 vjet pasi që kontrata të jetë ndryshuar apo të jetë ndërprerë.
   4. Të dhënat e referuara në pikën (1)(iii), (iv) dhe (v) do të ruhen të paktën për një periudhë prej 5 viteve.
   5. Të dhënat e referuara në pikën (1)(vi) do të ruhen deri sa ato ngjarje të sigurisë së informacionit të jenë rivlerësuar në përputhje me periodicitetin e definuar në një procedurë të themeluar nga organizata.
2. Organizata do të mbajë të dhëna për kualifikimin dhe përvojën e personelit të vet të përfshirë në aktivitetet e menaxhimit të sigurisë së informacionit
   1. Të dhënat mbi kualifikimet dhe përvojën e personelit duhet të ruhen për aq kohë sa personi punon për organizatën, dhe për të paktë 3 vite pasi që personi të ketë lënë organizatën.
   2. Anëtarëve të personelit, pas kërkesës nga ana e tyre, do t’iu jepet qasje në të dhënat e tyre individuale. Veç kësaj, pas kërkesës të tyre, organizata do t’ua ofrojë një kopje të të dhënave të tyre individuale me rastin e largimit nga organizata.
3. Formati i të dhënave do të specifikohet në procedurat e organizatës.
4. Të dhënat duhet të ruhen në një mënyrë që siguron mbrojtje nga dëmtimi, ndryshimi dhe vjedhja, duke përfshirë mundësinë e identifikimit të informacionit, kur kjo kërkohet, sipas nivelit të klasifikimit të sigurisë. Organizata do të sigurojë që të dhënat ruhen me përdorimin e mjeteve që siguron integritetin, autenticitetin dhe qasjen e autorizuar.

**IS.D.OR.250 Manuali për menaxhimin e sigurisë së informacionit (MMSI)**

1. Organizata do t'i vërë në dispozicion autoritetit kompetent një manual për menaxhimin e sigurisë së informacionit (MMSI) dhe, kur është e zbatueshme, çfarëdo manuali dhe procedurë të referuar, i cili përmban:
   1. një deklaratë të nënshkruar nga menaxheri përgjegjës ose, në rastin e organizatave projektuese, nga drejtuesi i organizatës së projektimit, që konfirmon se organizata do të punojë në çdo kohë në përputhje me këtë Shtojcë dhe me MMSI-në. Nëse menaxheri përgjegjës ose, në rastin e organizatave të projektimit, drejtuesi i organizatës së projektimit, nuk është Kryeshefi ekzekutiv (KE) i organizatës, atëherë edhe KE i tillë do ta nënshkruaj deklaratën(nënshkrimi i dytë në deklaratë);
   2. titullin(jtë), emrin(at), detyrat, llogaridhënien, përgjegjësitë dhe autorizimet e personit ose personave të referuar në pikën IS.D.OR.240(b) dhe (c);
   3. titullin, emrin, detyrat, llogaridhënien, përgjegjësitë dhe autorizimet e personit të përbashkët përgjegjës të referuar në pikën IS.D.OR.240(d), nëse është e zbatueshme;
   4. politikën e sigurisë së informacionit të organizatës të referuar në pikën IS.D.OR.200(a)(1);
   5. një përshkrim të përgjithshëm të numrit dhe kategorive të personelit dhe të sistemit në funksion për të planifikuar disponueshmërinë e personelit siç kërkohet nga pika IS.D.OR.240;
   6. titullin(jtë), emrin(at), detyrat, llogaridhëniet, përgjegjësitë dhe autorizimet e personave kyç përgjegjës për zbatimin e pikës IS.D.OR.200, përfshirë personin ose personat përgjegjës për monitorimin e funksionit të përputhshmërisë të referuar në pikën IS.D.OR.200(a)(12);
   7. një organigram që paraqet zinxhirët e ndërlidhur të llogaridhënies dhe përgjegjësisë për personat e referuar në pikat (2) dhe (6);
   8. përshkrimin e skemës së raportimit të brendshëm të referuar në pikën IS.D.OR.215;
   9. procedurat të cilat përcaktojnë se si organizata e siguron përputhshmërinë me këtë Pjesë, dhe në veçanti:
      1. dokumentacionin pika IS.D.OR.200(c);
      2. procedurat të cilat përcaktojnë se si e kontrollon organizata çfarëdo aktiviteti të kontraktuar të referuar në pikën IS.D. OR.200(a)(9);
      3. Procedurën për ndryshimin e MMSI-së të përcaktuar në pikën (c);
   10. Hollësitë mbi mjetet alternative të përputhshmërisë të miratuara aktualisht.
2. Versioni fillestar i nxjerrë i MMSI-së do të miratohet dhe një kopje do të ruhet nga autoriteti kompetent. MMSI do të ndryshohet sipas nevojës në mënyrë që të jetë një përshkrim i përditësuar i MMSI-së së organizatës. Një kopje e çfarëdo ndryshimi të MMSI-së do t'i ofrohet autoritetit kompetent.
3. Ndryshimet në MMSI do të menaxhohen në një procedurë të vendosur nga organizata. Çfarëdo ndryshimi që nuk përfshihet në fushëveprimin e kësaj procedure dhe çfarëdo ndryshimi në lidhje me ndryshimet e referuara në pikën IS.D. OR.255(b), do të miratohet nga autoriteti kompetent.
4. Organizata mund ta integrojë MMSI-në dokumentet e tjera shpjeguese të menaxhimit ose në manuale të tjera të menaxhimit të cilat ajo i mban, me kusht që të ketë një referencë tërthore e cila tregon se cilat pjesë të dokumentit shpjegues ose manualit të menaxhimit korrespondojnë me kërkesat e ndryshme të përfshira në këtë Shtojcë.

**IS.D.OR.255 Ndryshimet e sistemit të menaxhimit të sigurisë së informacionit**

1. Ndryshimet në SMSI mund të menaxhohen dhe për to t'i ofrohet njoftim autoritetit kompetent përmes një procedure të zhvilluar nga organizata. Kjo procedurë do miratohet nga autoriteti kompetent.
2. Në lidhje me ndryshimet në SMSI të cilat nuk mbulohen nga procedura e referuar në pikën (a), organizata duhet të parashtrojë kërkesë dhe të marrë një miratim të lëshuar nga autoriteti kompetent.

Në lidhje me këto ndryshimet:

* 1. kërkesa duhet të dorëzohet përpara se të ndodhë ndonjë ndryshim i tillë, në mënyrë që t'i mundësojë autoritetit kompetent të përcaktojë përputhshmërinë e vazhdueshme me këtë Rregullore dhe të ndryshojë, nëse është e nevojshme, certifikatën e organizatës dhe kushtet përkatëse të miratimit që ndërlidhen me të;
  2. organizata do t'i vej në dispozicion autoritetit kompetent çfarëdo informacioni që ai e kërkon për të vlerësuar ndryshimin;
  3. ndryshimi do të zbatohet vetëm pas marrjes së miratimit formal nga organi kompetent;
  4. organizata do të funksionojë sipas kushteve të përcaktuara nga organi kompetent gjatë zbatimit të ndryshimeve të tilla.

**IS.D.OR.260 Përmirësimi i vazhdueshëm**

1. Organizata do të vlerësojë, me përdorimin e treguesve adekuat të performancës, efektivitetin dhe maturitetin e SMSI-së. Ky vlerësim do të kryhet mbi një bazë kalendarike të paracaktuar nga organizata ose pas një incidenti të sigurisë së informacionit.
2. Në rast se konstatohen mangësi pas vlerësimit të kryer në përputhje me pikën (a), organizata do të ndërmerr masat e nevojshme të përmirësimit për të siguruar që SMSI të vazhdojë të jetë në përputhje me kërkesat e zbatueshme dhe që të mbajë rreziqet e sigurisë së informacionit në një nivel të pranueshëm. Përveç kësaj, organizata do të rivlerësojë ata elementë të SMSI-së të cilët preken nga masat e miratuara.

*ANNEX*

**INFORMATION SECURITY – ORGANISATION REQUIREMENTS**

**[PART-IS.D.OR]**

IS.D.OR.100 Scope

IS.D.OR.200 Information security management system IS.D.OR.205 Information security risk assessment IS.D.OR.210 Information security risk treatment IS.D.OR.215 Information security internal reporting scheme

IS.D.OR.220 Information security incidents – detection, response, and recovery IS.D.OR.225 Response to findings notified by the competent authority IS.D.OR.230 Information security external reporting scheme

IS.D.OR.235 Contracting of information security management activities IS.D.OR.240 Personnel requirements

IS.D.OR.245 Record-keeping

IS.D.OR.250 Information security management manual (ISMM) IS.D.OR.255 Changes to the information security management system IS.D.OR.260 Continuous improvement

**IS.D.OR.100 Scope**

This Part establishes the requirements to be met by the organisations referred to in Article 2 of this Regulation.

**IS.D.OR.200 Information security management system (ISMS)**

1. In order to achieve the objectives set out in Article 1, the organisation shall set up, implement and maintain an information security management system (ISMS) which ensures that the organisation:
   1. establishes a policy on information security setting out the overall principles of the organisation with regard to the potential impact of information security risks on aviation safety;
   2. identifies and reviews information security risks in accordance with point IS.D.OR.205;
   3. defines and implements information security risk treatment measures in accordance with point IS.D.OR.210;
   4. implements an information security internal reporting scheme in accordance with point IS.D.OR.215;
   5. defines and implements, in accordance with point IS.D.OR.220, the measures required to detect information security events, identifies those events which are considered incidents with a potential impact on aviation safety except as permitted by point IS.D.OR.205(e), and responds to, and recovers from, those information security incidents;
   6. implements the measures that have been notified by the competent authority as an immediate reaction to an information security incident or vulnerability with an impact on aviation safety;
   7. takes appropriate action, in accordance with point IS.D.OR.225, to address findings notified by the competent authority;
   8. implements an external reporting scheme in accordance with point IS.D.OR.230 in order to enable the competent authority to take appropriate actions;
   9. complies with the requirements contained in point IS.D.OR.235 when contracting any part of the activities referred to in point IS.D.OR.200 to other organisations;
   10. complies with the personnel requirements laid down in point IS.D.OR.240;
   11. complies with the record-keeping requirements laid down in point IS.D.OR.245;
   12. monitors compliance of the organisation with the requirements of this Regulation and provides feedback on findings to the accountable manager or, in the case of design organisations, to the head of the design organisation, in order to ensure effective implementation of corrective actions;
   13. protects, without prejudice to applicable incident reporting requirements, the confidentiality of any information that the organisation may have received from other organisations, according to its level of sensitivity.
2. In order to continuously meet the requirements referred to in Article 1, the organisation shall implement a continuous improvement process in accordance with point IS.D.OR.260.
3. The organisation shall document, in accordance with point IS.D.OR.250, all key processes, procedures, roles and responsibilities required to comply with point IS.D.OR.200(a) and establish a process for amending that documentation. Changes to those processes, procedures, roles and responsibilities shall be managed in accordance with point IS.D.OR.255.
4. The processes, procedures, roles and responsibilities established by the organisation in order to comply with point IS.D. OR.200(a) shall correspond to the nature and complexity of its activities, based on an assessment of the information security risks inherent to those activities, and may be integrated within other existing management systems already implemented by the organisation.
5. Without prejudice to the obligation to comply with the reporting requirements contained Regulation (CAA) no. 09/2017 on the reporting, analysis and follow-up of occurrences in civil aviation and the requirements of point IS.D.OR.200 (a) (13), the organisation may be granted approval by the competent authority not to implement the requirements referred to in points (a) to (d)) and the related requirements contained in points IS.D.OR.205 through IS.D.OR.260, if it demonstrates to the satisfaction of that authority that its activities, facilities and resources, as well as the services it operates, provides, receives and maintains, do not pose any information security risks with a potential impact on aviation safety neither to itself nor to other organisations. The approval shall be based on a documented information security risk assessment carried out by the organisation or a third party in accordance with point IS.D.OR.205 and reviewed and approved by its competent authority.

The continued validity of that approval will be reviewed by the competent authority following the applicable oversight audit cycle and whenever changes are implemented in the scope of work of the organisation.

**IS.D.OR.205 Information security risk assessment**

1. The organisation shall identify all of its elements, which could be exposed to information security risks. That shall include:
   1. the organisation’s activities, facilities and resources, as well as the services the organisation operates, provides, receives or maintains;
   2. the equipment, systems, data and information that contribute to the functioning of the elements listed in point (1).
2. The organisation shall identify the interfaces that it has with other organisations, and which could result in the mutual exposure to information security risks.
3. With regard to the elements and interfaces referred to in points (a) and (b), the organisation shall identify the information security risks which may have a potential impact on aviation safety. For each identified risk, the organisation shall:
   1. assign a risk level according to a predefined classification established by the organisation;
   2. associate each risk and its level with the corresponding element or interface identified in accordance with points (a) and (b).

The predefined classification referred to in point (1) shall take into account the potential of occurrence of the threat scenario and the severity of its safety consequences. Based on that classification, and taking into account whether the organisation has a structured and repeatable risk management process for operations, the organisation shall be able to establish whether the risk is acceptable or needs to be treated in accordance with point IS.D.OR.210.

In order to facilitate the mutual comparability of risks assessments, the assignment of the risk level pursuant to point

1. shall take into account relevant information acquired in coordination with the organisations referred to in point (b).
2. The organisation shall review and update the risk assessment carried out in accordance with points (a), (b) and (c) in any of the following situations:
   1. there is a change in the elements subject to information security risks;
   2. there is a change in the interfaces between the organisation and other organisations, or in the risks communicated by the other organisations;
   3. there is a change in the information or knowledge used for the identification, analysis and classification of risks;
   4. there are lessons learnt from the analysis of information security incidents.

**IS.D.OR.210 Information security risk treatment**

1. The organisation shall develop measures to address unacceptable risks identified in accordance with point IS.D. OR.205, implement them in a timely manner and check their continued effectiveness. Those measures shall enable the organisation to:
   1. control the circumstances that contribute to the effective occurrence of the threat scenario;
   2. reduce the consequences on aviation safety associated with the materialisation of the threat scenario;
   3. avoid the risks.

Those measures shall not introduce any new potential unacceptable risks to aviation safety.

1. The person referred to in point IS.D.OR.240 (a) and (b) and other affected personnel of the organisation shall be informed of the outcome of the risk assessment carried out in accordance with point IS.D.OR.205, the corresponding threat scenarios and the measures to be implemented.

The organisation shall also inform organisations with which it has an interface in accordance with point IS.D.OR.205

(b) of any risk shared between both organisations.

**IS.D.OR.215 Information security internal reporting scheme**

1. The organisation shall establish an internal reporting scheme to enable the collection and evaluation of information security events, including those to be reported pursuant to point IS.D.OR.230.
2. That scheme and the process referred to in point IS.D.OR.220 shall enable the organisation to:
   1. identify which of the events reported pursuant to point (a) are considered information security incidents or vulnerabilities with a potential impact on aviation safety;
   2. identify the causes of, and contributing factors to, the information security incidents and vulnerabilities identified in accordance with point (1), and address them as part of the information security risk management process in accordance with points IS.D.OR.205 and IS.D.OR.220;
   3. ensure an evaluation of all known, relevant information relating to the information security incidents and vulnerabilities identified in accordance with point (1);
   4. ensure the implementation of a method to distribute internally the information as necessary.
3. Any contracted organisation which may expose the organisation to information security risks with a potential impact on aviation safety shall be required to report information security events to the organisation. Those reports shall be submitted using the procedures established in the specific contractual arrangements and shall be evaluated in accordance with point (b).
4. The organisation shall cooperate on investigations with any other organisation that has a significant contribution to the information security of its own activities.
5. The organisation may integrate that reporting scheme with other reporting schemes it has already implemented.

**IS.D.OR.220 Information security incidents – detection, response and recovery**

1. Based on the outcome of the risk assessment carried out in accordance with point IS.D.OR.205 and the outcome of the risk treatment performed in accordance with point IS.D.OR.210, the organisation shall implement measures to detect incidents and vulnerabilities that indicate the potential materialisation of unacceptable risks and which may have a potential impact on aviation safety. Those detection measures shall enable the organisation to:
   1. identify deviations from predetermined functional performance baselines;
   2. trigger warnings to activate proper response measures, in case of any deviation.
2. The organisation shall implement measures to respond to any event conditions identified in accordance with point (a) that may develop or have developed into an information security incident. Those response measures shall enable the organisation to:
   1. initiate the reaction to the warnings referred to in point (a)(2) by activating predefined resources and course of actions;
   2. contain the spread of an attack and avoid the full materialisation of a threat scenario;
   3. control the failure mode of the affected elements defined in point IS.D.OR.205(a).
3. The organisation shall implement measures aimed at recovering from information security incidents, including emergency measures, if needed. Those recovery measures shall enable the organisation to:
   1. remove the condition that caused the incident, or constrain it to a tolerable level;
   2. reach a safe state of the affected elements defined in point IS.D.OR.205(a) within a recovery time previously defined by the organisation.

**IS.D.OR.225 Response to findings notified by the competent authority**

1. After receipt of the notification of findings submitted by the competent authority, the organisation shall:
   1. identify the root cause or causes of, and contributing factors to, the non-compliance;
   2. define a corrective action plan;
   3. demonstrate the correction of the non-compliance to the satisfaction of the competent authority.
2. The actions referred to in point (a) shall be carried out within the period agreed with the competent authority.

**IS.D.OR.230 Information security external reporting scheme**

1. The organisation shall implement an information security reporting system that complies with the requirements laid down in Regulation (CAA) no. 09/2017 and its amendments, if applicable to the organisation.
2. Without prejudice to the obligations of Regulation (CAA) no. 09/2017, the organisation shall ensure that any information security incident or vulnerability, which may represent a significant risk to aviation safety, is reported to their competent authority. Furthermore:
   1. where such an incident or vulnerability affects an aircraft or associated system or component, the organisation shall also report it to the design approval holder;
   2. where such an incident or vulnerability affects a system or constituent used by the organisation, the organisation shall report it to the organisation responsible for the design of the system or constituent.
3. The organisation shall report the conditions referred to in point (b) as follows:
   1. a notification shall be submitted to the competent authority and, if applicable, to the design approval holder or to the organisation responsible for the design of the system or constituent, as soon as the condition has been known to the organisation;
   2. a report shall be submitted to the competent authority and, if applicable, to the design approval holder or to the organisation responsible for the design of the system or constituent, as soon as possible, but not exceeding 72 hours from the time the condition has been known to the organisation, unless exceptional circumstances prevent this.

The report shall be made in the form defined by the competent authority and shall contain all relevant information about the condition known to the organisation;

* 1. a follow-up report shall be submitted to the competent authority and, if applicable, to the design approval holder or to the organisation responsible for the design of the system or constituent, providing details of the actions the organisation has taken or intends to take to recover from the incident and the actions it intends to take to prevent similar information security incidents in the future.

The follow-up report shall be submitted as soon as those actions have been identified, and shall be produced in the form defined by the competent authority.

**IS.D.OR.235 Contracting of information security management activities**

1. The organisation shall ensure that when contracting any part of the activities referred to in point IS.D.OR.200 to other organisations, the contracted activities comply with the requirements of this Regulation and the contracted organisation works under its oversight. The organisation shall ensure that the risks associated with the contracted activities are appropriately managed.
2. The organisation shall ensure that the competent authority can have access upon request to the contracted organisation to determine continued compliance with the applicable requirements laid down in this Regulation.

**IS.D.OR.240 Personnel requirements**

1. The accountable manager of the organisation or, in the case of design organisations, the head of the design organisation, designated in accordance with Regulation (CAA) No. 06/2015 and Regulation (CAA) No. 17/2017 as referred to in points 1(a) and (b) of Article 2 of this Regulation, shall have corporate authority to ensure that all activities required by this Regulation can be financed and carried out. That person shall:
   1. ensure that all necessary resources are available to comply with the requirements of this Regulation;
   2. establish and promote the information security policy referred to in point IS.D.OR.200(a)(1);
   3. demonstrate a basic understanding of this Regulation.
2. The accountable manager or, in the case of design organisations, the head of the design organisation, shall appoint a person or group of persons to ensure that the organisation is in compliance with the requirements of this Regulation, and shall define the extent of their authority. That person or group of persons shall report directly to the accountable manager or, in the case of design organisations, to the head of the design organisation, and shall have the appropriate knowledge, background and experience to discharge their responsibilities. It shall be determined in the procedures who deputises for a particular person in the case of lengthy absence of that person.
3. The accountable manager or, in the case of design organisations, the head of the design organisation shall appoint a person or group of persons with the responsibility to manage the compliance monitoring function referred to in point IS.D.OR.200(a)(12).
4. Where the organisation shares information security organisational structures, policies, processes and procedures, with other organisations or with areas of their own organisation which are not part of the approval or declaration, the accountable manager or, in the case of design organisations, the head of the design organisation, may delegate its activities to a common responsible person.

In such a case, coordination measures shall be established between the accountable manager of the organisation or, in the case of design organisations, the head of the design organisation, and the common responsible person to ensure adequate integration of the information security management within the organisation.

1. The accountable manager or the head of the design organisation, or the common responsible person referred to in point (d), shall have corporate authority to establish and maintain the organisational structures, policies, processes and procedures necessary to implement point IS.D.OR.200.
2. The organisation shall have a process in place to ensure that they have sufficient personnel on duty to carry out the activities covered by this Annex.
3. The organisation shall have a process in place to ensure that the personnel referred to in point (f) have the necessary competence to perform their tasks.
4. The organisation shall have a process in place to ensure that personnel acknowledge the responsibilities associated with the assigned roles and tasks.
5. The organisation shall ensure that the identity and trustworthiness of the personnel who have access to information systems and data subject to the requirements of this Regulation are appropriately established.

**IS.D.OR.245 Record-keeping**

1. The organisation shall keep records of its information security management activities
   1. The organisation shall ensure that the following records are archived and traceable:
      1. any approval received and any associated information security risk assessment in accordance with point IS.D. OR.200(e);
      2. contracts for activities referred to in point IS.D.OR.200(a)(9);
      3. records of the key processes referred to in point IS.D.OR.200(d);
      4. records of the risks identified in the risk assessment referred to in point IS.D.OR.205 along with the associated risk treatment measures referred to in point IS.D.OR.210;
      5. records of information security incidents and vulnerabilities reported in accordance with the reporting schemes referred to in points IS.D.OR.215 and IS.D.OR.230;
      6. records of those information security events which may need to be reassessed to reveal undetected information security incidents or vulnerabilities.
   2. The records referred to in point (1)(i) shall be retained at least until 5 years after the approval has lost its validity.
   3. The records referred to in point (1)(ii) shall be retained at least until 5 years after the contract has been amended or terminated.
   4. The records referred to in point (1)(iii), (iv) and (v) shall be retained at least for a period of 5 years.
   5. The records referred to in point (1)(vi) shall be retained until those information security events have been reassessed in accordance with a periodicity defined in a procedure established by the organisation.
2. The organisation shall keep records of qualification and experience of its own staff involved in information security management activities
   1. The personnel’s qualification and experience records be retained for as long as the person works for the organisation, and for at least 3 years after the person has left the organisation.
   2. Members of the staff shall, upon their request, be given access to their individual records. In addition, upon their request, the organisation shall provide them with a copy of their individual records on leaving the organisation.
3. The format of the records shall be specified in the organisation’s procedures.
4. Records shall be stored in a manner that ensures protection from damage, alteration and theft, with information being identified, when required, according to its security classification level. The organisation shall ensure that the records are stored using means to ensure integrity, authenticity and authorised access.

**IS.D.OR.250 Information security management manual (ISMM)**

1. The organisation shall make available to the competent authority an information security management manual (ISMM) and, where applicable, any referenced associated manuals and procedures, containing:
   1. a statement signed by the accountable manager or, in the case of design organisations, by the head of the design organisation, confirming that the organisation will at all times work in accordance with this Annex and with the ISMM. If the accountable manager or, in the case of design organisations, the head of the design organisation, is not the chief executive officer (CEO) of the organisation, then such CEO shall countersign the statement;
   2. the title(s), name(s), duties, accountabilities, responsibilities and authorities of the person or persons referred to in point IS.D.OR.240(b) and (c);
   3. the title, name, duties, accountabilities, responsibilities and authorities of the common responsible person referred to in point IS.D.OR.240(d), if applicable;
   4. the information security policy of the organisation as referred to in point IS.D.OR.200(a)(1);
   5. a general description of the number and categories of staff and of the system in place to plan the availability of staff as required by point IS.D.OR.240;
   6. the title(s), name(s), duties, accountabilities, responsibilities and authorities of the key persons responsible for the implementation of point IS.D.OR.200, including the person or persons responsible for the compliance monitoring function referred to in point IS.D.OR.200(a)(12);
   7. an organisation chart showing the associated chains of accountability and responsibility for the persons referred to in points (2) and (6);
   8. the description of the internal reporting scheme referred to in point IS.D.OR.215;
   9. the procedures that specify how the organisation ensures compliance with this Part, and in particular:
      1. the documentation point IS.D.OR.200(c);
      2. the procedures that define how the organisation controls any contracted activities referred to in point IS.D. OR.200(a)(9);
      3. the ISMM amendment procedure defined in point (c);
   10. the details of currently approved alternative means of compliance.
2. The initial issue of the ISMM shall be approved and a copy shall be retained by the competent authority. The ISMM shall be amended as necessary to remain an up-to-date description of the ISMS of the organisation. A copy of any amendments to the ISMM shall be provided to the competent authority.
3. Amendments to the ISMM shall be managed in a procedure established by the organisation. Any amendments that are not included within the scope of this procedure and any amendments related to the changes referred to in point IS.D. OR.255(b), shall be approved by the competent authority.
4. The organisation may integrate the ISMM with other management expositions or manuals it holds, provided there is a clear cross reference that indicates which portions of the management exposition or manual correspond to the different requirements contained in this Annex.

**IS.D.OR.255 Changes to the information security management system**

1. Changes to the ISMS may be managed and notified to the competent authority in a procedure developed by the organisation. This procedure shall be approved by the competent authority.
2. With regard to changes to the ISMS not covered by the procedure referred to in point (a), the organisation shall apply for and obtain an approval issued by the competent authority.

With regard to these changes:

* 1. the application shall be submitted before any such change takes place, in order to enable the competent authority to determine continued compliance with this Regulation and to amend, if necessary, the organisation certificate and related terms of approval attached to it;
  2. the organisation shall make available to the competent authority any information it requests to evaluate the change;
  3. the change shall be implemented only upon receipt of a formal approval by the competent authority;
  4. the organisation shall operate under the conditions prescribed by the competent authority during the implementation of such changes.

**IS.D.OR.260 Continuous improvement**

1. The organisation shall assess, using adequate performance indicators, the effectiveness and maturity of the ISMS. That assessment shall be carried out on a calendar basis predefined by the organisation or following an information security incident.
2. If deficiencies are found following the assessment carried out in accordance with point (a), the organisation shall take the necessary improvement measures to ensure that the ISMS continues to comply with the applicable requirements and maintains the information security risks at an acceptable level. In addition, the organisation shall reassess those elements of the ISMS affected by the adopted measures.

*ANEKS*

**BEZBEDNOST INFORMACIJA – ZAHTEVI ORGANIZACIJE**

**[DEO-IS.D.OR]**

„IS.D.OR.100 Delokrug

IS.D.OR.200 Sistem upravljanja bezbednošću informacija IS.D.OR.205 Procena rizika po bezbednost informacija IS.D.OR.210 Tretman rizika po bezbednost informacija IS.D.OR.215 Interna šema izveštavanja o bezbednosti informacija

IS.D.OR.220 Incidenti bezbednosti informacija – otkrivanje, odgovor i oporavak IS.D.OR.225 Odgovor na nalaze koje je saopštio nadležni organ IS.D.OR.230 Šema eksternog izveštavanja o bezbednosti informacija

IS.D.OR.235 Ugovaranje aktivnosti upravljanja bezbednošću informacija IS.D.OR.240 Potrebe za osobljem

IS.D.OR.245 Vođenje evidencije

IS.D.OR.250 Priručnik za upravljanje bezbednošću informacija (PUBI) IS.D.OR.255 Promene sistema upravljanja bezbednošću informacija IS.D.OR.260 Kontinuirano unapređenje

**„IS.D.OR.100 Delokrug**

Ovim delom se utvrđuju zahtevi koje moraju da ispune organizacije navedene u članu 2. ove uredbe.

**IS.D.OR.200 Sistem upravljanja bezbednošću informacija (SUBI)**

1. Da bi se postigli ciljevi navedeni u članu 1, organizacija će uspostaviti, implementirati i održavati sistem upravljanja bezbednošću informacija (SUBI) koji osigurava da organizacija:
   1. uspostavlja politiku o bezbednosti informacija kojom se utvrđuju opšti principi organizacije u pogledu potencijalnog uticaja rizika bezbednosti informacija na bezbednost vazduhoplovstva;
   2. identifikuje i preispituje rizike po bezbednost informacija u skladu sa tačkom IS.D.OR.205;
   3. definiše i sprovodi mere za tretman rizika bezbednosti informacija u skladu sa tačkom IS.D.OR.210;
   4. implementira internu šemu izveštavanja o bezbednosti informacija u skladu sa tačkom IS.D.OR.215;
   5. definiše i sprovodi, u skladu sa tačkom IS.D.OR.220, mere potrebne za otkrivanje događaja u vezi sa informacionom bezbednošću, identifikuje one događaje koji se smatraju incidentima sa potencijalnim uticajem na bezbednost vazduhoplovstva, osim kako je dozvoljeno tačkom IS.D.OR.205(e), i reaguje na te incidente u vezi sa informacionom bezbednošću i oporavlja se od njih;
   6. sprovodi mere koje je nadležni organ obavestio kao neposrednu reakciju na incident ili ranjivost u vezi sa informacionom bezbednošću sa uticajem na bezbednost vazduhoplovstva;
   7. preduzima odgovarajuće mere, u skladu sa tačkom IS.D.OR.225, kako bi se pozabavio nalazima koje je saopštio nadležni organ;
   8. sprovodi eksterni sistem izveštavanja u skladu sa tačkom IS.D.OR.230 kako bi nadležni organ mogao da preduzme odgovarajuće mere;
   9. ispunjava zahteve sadržane u tački IS.D.OR.235, prilikom ugovaranja bilo kog dela aktivnosti navedenih u tački IS.D.OR.200 sa drugim organizacijama;
   10. ispunjava zahteve za osoblje utvrđene u tački IS.D.OR.240;
   11. ispunjava zahteve za vođenje evidencije utvrđene u tački IS.D.OR.245;
   12. prati usklađenost organizacije sa zahtevima ovog pravilnika i pruža povratne informacije o nalazima odgovornom rukovodiocu ili, u slučaju projektantskih organizacija, rukovodiocu projektantske organizacije, kako bi se osigurala efikasna primena korektivnih mera;
   13. štiti, bez obzira na važeće zahteve za izveštavanje o incidentima, poverljivost bilo koje informacije koju je organizacija mogla da primi od drugih organizacija, u skladu sa nivoom njene osetljivosti.
2. Da bi kontinuirano ispunjavala zahteve iz člana 1, organizacija mora da sprovodi proces kontinuiranog poboljšanja u skladu sa tačkom IS.D.OR.260.
3. Organizacija mora da dokumentuje, u skladu sa tačkom IS.D.OR.250, sve ključne procese, procedure, uloge i odgovornosti potrebne za usklađivanje sa tačkom IS.D.OR.200(a) i da uspostavi postupak za izmenu te dokumentacije. Promene tih procesa, procedura, uloga i odgovornosti upravljaju se u skladu sa tačkom IS.D.OR.255.
4. Procesi, procedure, uloge i odgovornosti koje je organizacija uspostavila kako bi se uskladila sa tačkom IS.D. OR.200(a) mora odgovarati prirodi i složenosti njenih aktivnosti, na osnovu procene rizika po bezbednost informacija, svojstvenih tim aktivnostima, i može se integrisati u druge postojeće sisteme upravljanja koje je organizacija već implementirala.
5. Bez obzira na obavezu poštovanja zahteva za izveštavanje sadržanih u Uredbi (ACV) br. 09/2017 o izveštavanju, analizi i praćenju događaja u civilnom vazduhoplovstvu i zahteva iz tačke IS.D.OR.200 (a) (13), organizacija može dobiti odobrenje od strane nadležnog organa da ne sprovodi zahteve iz tačaka (a) do (d)) i povezane zahteve sadržane u tačkama IS.D.OR.205 do IS.D.OR.260, ako zadovoljavajuće dokaže tom organu da njene aktivnosti, objekti i resursi, kao i usluge koje posluje, pruža, prima i održava, ne predstavljaju nikakve rizike po bezbednost informacija sa potencijalnim uticajem na bezbednost vazduhoplovstva, kako za nju samu tako ni za druge organizacije. Odobrenje se zasniva na dokumentovanoj proceni rizika po bezbednost informacija koju sprovodi organizacija ili treća strana u skladu sa tačkom IS.D.OR.205, a koju pregleda i odobri njen nadležni organ.

Nadležni organ će preispitati kontinuiranu važnost tog odobrenja nakon važećeg ciklusa nadzorne revizije i kad god se promene sprovedu u obimu rada organizacije.

**IS.D.OR.205 Procena rizika po bezbednost informacija**

1. Organizacija mora da identifikuje sve svoje elemente koji bi mogli biti izloženi rizicima po bezbednost informacija. To će uključivati:
   1. aktivnosti, objekte i resurse organizacije, kao i usluge koje organizacija posluje, pruža, prima ili održava;
   2. opremu, sisteme, podatke i informacije koje doprinose funkcionisanju elemenata navedenih u tački (1).
2. Organizacija mora da identifikuje interfejse koje ima sa drugim organizacijama, a koji bi mogli dovesti do obostranog izlaganja rizicima bezbednosti informacija.
3. U vezi sa elementima i interfejsima navedenim u tačkama (a) i (b), organizacija mora da identifikuje rizike po bezbednost informacija, koji mogu imati potencijalni uticaj na bezbednost vazduhoplovstva. Za svaki identifikovani rizik, organizacija će:
   1. dodeliti nivo rizika prema unapred definisanoj klasifikaciji koju je utvrdila organizacija;
   2. povezati svaki rizik i njegov nivo sa odgovarajućim elementom ili interfejsom identifikovanim u skladu sa tačkama (a) i (b).

Unapred definisana klasifikacija navedena u tački (1) uzima u obzir mogućnost pojave scenarija pretnje i ozbiljnost njegovih bezbednosnih posledica. Na osnovu te klasifikacije, i uzimajući u obzir da li organizacija ima strukturiran i ponovljiv proces upravljanja rizicima za operacije, organizacija mora biti u stanju da utvrdi da li je rizik prihvatljiv ili ga je potrebno tretirati u skladu sa tačkom IS.D.OR.210.

Radi olakšavanja međusobne uporedivosti procena rizika, dodeljivanje nivoa rizika u skladu sa tačkom

1. uzeće u obzir relevantne informacije prikupljene u koordinaciji sa organizacijama navedenim u tački (b).
2. Organizacija će preispitati i ažurirati procenu rizika sprovedenu u skladu sa tačkama (a), (b) i (c) u bilo kojoj od sledećih situacija:
   1. došlo je do promene elemenata koji su podložni rizicima po bezbednost informacija;
   2. došlo je do promene u interfejsima između organizacije i drugih organizacija ili u rizicima koje su saopštile druge organizacije;
   3. došlo je do promene informacija ili znanja koje se koristi za identifikaciju, analizu i klasifikaciju rizika;
   4. postoje lekcije naučene iz analize incidenata u vezi sa informacionom bezbednošću.

**IS.D.OR.210 Tretman rizika po bezbednost informacija**

1. Organizacija mora da razvije mere za rešavanje neprihvatljivih rizika identifikovanih u skladu sa tačkom IS.D. OR.205, blagovremeno ih sprovede i proveri njihovu kontinuiranu efikasnost. Te mere će omogućiti organizaciji da:
   1. kontroliše okolnosti koje doprinose efektivnom nastanku scenarija pretnje;
   2. smanji posledice po bezbednost vazduhoplovstva povezane sa ostvarivanjem scenarija pretnje;
   3. izbegne rizike.

Te mere ne smeju uvoditi nikakve nove potencijalne neprihvatljive rizike za bezbednost vazduhoplovstva.

1. Lice navedeno u tački IS.D.OR.240 (a) i (b) i ostalo pogođeno osoblje organizacije moraju biti obavešteni o ishodu procene rizika, sprovedene u skladu sa tačkom IS.D.OR.205, odgovarajućim scenarijima pretnji i merama koje treba sprovesti.

Organizacija takođe obaveštava organizacije sa kojima ima interfejs u skladu sa tačkom IS.D.OR.205

(b) o bilo kojem riziku koji dele obe organizacije.

**IS.D.OR.215 Interna šema izveštavanja o bezbednosti informacija**

1. Organizacija mora da uspostavi interni sistem izveštavanja kako bi omogućila prikupljanje i procenu događaja u vezi sa informacionom bezbednošću, uključujući i one koji se prijavljuju u skladu sa tačkom IS.D.OR.230.
2. Ta šema i proces naveden u tački IS.D.OR.220 moraju omogućiti organizaciji da:
   1. utvrdi koji od događaja prijavljenih u skladu sa tačkom (a) se smatraju incidentima ili ranjivostima u vezi sa bezbednošću informacija sa potencijalnim uticajem na bezbednost vazduhoplovstva;
   2. identifikuje uzroke i faktore koji doprinose incidentima i ranjivostima u vezi sa bezbednošću informacija identifikovanim u skladu sa tačkom (1), i reši ih kao deo procesa upravljanja rizicima u vezi sa bezbednošću informacija u skladu sa tačkama IS.D.OR.205 i IS.D.OR.220;
   3. obezbedi procenu svih poznatih, relevantnih informacija koje se odnose na incidente i ranjivosti u vezi sa bezbednošću informacija identifikovanih u skladu sa tačkom (1);
   4. obezbedi implementaciju metode za internu distribuciju informacija po potrebi.
3. Svaka ugovorna organizacija koja može izložiti organizaciju rizicima u vezi sa informacionom bezbednošću sa potencijalnim uticajem na bezbednost vazduhoplovstva biće dužna da prijavi događaje u vezi sa informacionom bezbednošću organizaciji. Ti izveštaji se podnose korišćenjem procedura utvrđenih u posebnim ugovornim aranžmanima i ocenjuju se u skladu sa tačkom (b).
4. Organizacija će sarađivati u istragama sa bilo kojom drugom organizacijom koja ima značajan doprinos bezbednosti informacija njenih sopstvenih aktivnosti.
5. Organizacija može integrisati tu šemu izveštavanja sa drugim šemama izveštavanja koje je već implementirala.

**IS.D.OR.220 Incidenti bezbednosti informacija – otkrivanje, odgovor i oporavak**

1. Na osnovu rezultata procene rizika sprovedene u skladu sa tačkom IS.D.OR.205 i rezultata tretmana rizika sprovedenog u skladu sa tačkom IS.D.OR.210, organizacija mora da sprovede mere za otkrivanje incidenata i ranjivosti koje ukazuju na potencijalnu materijalizaciju neprihvatljivih rizika i koje mogu imati potencijalni uticaj na bezbednost vazduhoplovstva. Te mere otkrivanja moraju omogućiti organizaciji da:
   1. identifikuje odstupanja od unapred određenih osnovnih funkcionalnih performansi;
   2. pokrene upozorenja kako bi se aktivirale odgovarajuće mere reagovanja, u slučaju bilo kakvog odstupanja.
2. Organizacija mora da sprovede mere za reagovanje na sve događaje identifikovane u skladu sa tačkom (a) koji mogu da se razviju ili su se razvili u incident bezbednosti informacija. Te mere reagovanja moraju omogućiti organizaciji da:
   1. pokrene reakciju na upozorenja iz tačke (a)(2) aktiviranjem unapred definisanih resursa i toka delovanja;
   2. obuzda širenje napada i sprečiti potpunu materijalizaciju scenarija pretnje;
   3. kontroliše način otkaza pogođenih elemenata definisanih u tački IS.D.OR.205(a).
3. Organizacija će sprovesti mere usmerene na oporavak od incidenata bezbednosti informacija, uključujući i hitne mere, ako je potrebno. Te mere oporavka moraju omogućiti organizaciji da:
   1. otkloni uslov koji je izazvao incident ili ga ograničiti na podnošljiv nivo;
   2. dostigne bezbedno stanje pogođenih elemenata definisanih u tački IS.D.OR.205(a) u vremenskom roku oporavka koje je prethodno definisala organizacija.

**IS.D.OR.225 Odgovor na nalaze koje je saopštio nadležni organ**

1. Nakon prijema obaveštenja o nalazima koje je podneo nadležni organ, organizacija je dužna da:
   1. identifikuje osnovni uzrok ili uzroke neusaglašenosti i faktore koji doprinose njoj;
   2. definiše plan korektivnih akcija;
   3. dokaže ispravku neusaglašenosti na zadovoljavajući način za nadležni organ.
2. Radnje navedene u tački (a) sprovode se u roku dogovorenom sa nadležnim organom.

**IS.D.OR.230 Šema eksternog izveštavanja o bezbednosti informacija**

1. Organizacija mora da implementira sistem izveštavanja o bezbednosti informacija koji je u skladu sa zahtevima utvrđenim Uredbom (ACV) br. 09/2017 i njenim izmenama i dopunama, ako je primenljivo na organizaciju.
2. Bez obzira na obaveze iz Uredbe (ACV) br. 09/2017, organizacija mora da obezbedi da se svaki incident ili ranjivost u vezi sa bezbednošću informacija, koji mogu predstavljati značajan rizik za bezbednost vazduhoplovstva, prijavi njihovom nadležnom organu. Dalje:
   1. kada takav incident ili ranjivost utiče na vazduhoplov ili povezani sistem ili komponentu, organizacija je dužna da to prijavi i nosiocu odobrenja projekta;
   2. Ukoliko takav incident ili ranjivost utiče na sistem ili komponentu koju koristi organizacija, organizacija je dužna da to prijavi organizaciji odgovornoj za projektovanje sistema ili komponente.
3. Organizacija je dužna da prijavi uslove navedene u tački (b) na sledeći način:
   1. Obaveštenje se dostavlja nadležnom organu i, ako je primenljivo, nosiocu odobrenja projekta ili organizaciji odgovornoj za projektovanje sistema ili komponente, čim organizacija sazna za stanje;
   2. Izveštaj se podnosi nadležnom organu i, ako je primenljivo, nosiocu odobrenja projekta ili organizaciji odgovornoj za projektovanje sistema ili komponente, što je pre moguće, ali ne duže od 72 sata od trenutka kada je organizacija saznala za stanje, osim ako izuzetne okolnosti to sprečavaju.

Izveštaj se sastavlja u formi koju je definisao nadležni organ i sadrži sve relevantne informacije o stanju koje je poznato organizaciji;

* 1. Nadležnom organu i, ako je primenljivo, nosiocu odobrenja za projektovanje ili organizaciji, odgovornoj za projektovanje sistema ili komponente, dostavlja se izveštaj o naknadnim aktivnostima u kojem se navode detalji o merama koje je organizacija preduzela ili namerava da preduzme da bi se oporavila od incidenta i merama koje namerava da preduzme da bi sprečila slične incidente u vezi sa bezbednošću informacija u budućnosti.

Izveštaj o praćenju se podnosi čim se te radnje identifikuju i izrađuje se u formi koju je definisao nadležni organ.

**IS.D.OR.235 Ugovaranje aktivnosti upravljanja bezbednošću informacija**

1. Organizacija mora da obezbedi da prilikom ugovaranja bilo kog dela aktivnosti navedenih u tački IS.D.OR.200 sa drugim organizacijama, ugovorene aktivnosti ispunjavaju zahteve ove uredbe i da ugovorena organizacija radi pod njenim nadzorom. Organizacija mora da obezbedi da se rizici povezani sa ugovorenim aktivnostima upravljaju na odgovarajući način.
2. Organizacija mora da obezbedi da nadležni organ može imati pristup na zahtev ugovornoj organizaciji kako bi utvrdio kontinuiranu ispunjenost važećih zahteva utvrđenih ovom Uredbom.

**IS.D.OR.240 Zahtevi za osoblje**

1. Odgovorni rukovodilac organizacije ili, u slučaju projektantskih organizacija, rukovodilac projektantske organizacije, imenovan u skladu sa Uredbom (ACV) br. 06/2015 i Uredbom (ACV) br. 17/2017 kako je navedeno u tačkama 1(a) i (b) člana 2 ove Uredbe, ima korporativno ovlašćenje da osigura da se sve aktivnosti koje zahteva ova Uredba mogu finansirati i sprovesti. Ta osoba će:
   1. osigurati da su svi potrebni resursi dostupni za ispunjavanje zahteva ove uredbe;
   2. uspostaviti i promovisati politiku bezbednosti informacija navedenu u tački IS.D.OR.200(a)(1);
   3. pokazati osnovno razumevanje ove Uredbe.
2. Odgovorni rukovodilac ili, u slučaju projektantskih organizacija, rukovodilac projektantske organizacije, imenuje lice ili grupu lica kako bi se osiguralo da organizacija ispunjava zahteve ove Uredbe i definiše obim njihovih ovlašćenja. To lice ili grupa lica direktno izveštava odgovornom rukovodiocu ili, u slučaju projektantskih organizacija, rukovodiocu projektantske organizacije, i poseduje odgovarajuće znanje, iskustvo i stručnost za obavljanje svojih odgovornosti. U postupku se utvrđuje ko zamenjuje određeno lice u slučaju dužeg odsustva tog lica.
3. Odgovorni rukovodilac ili, u slučaju projektantskih organizacija, rukovodilac projektantske organizacije, imenuje lice ili grupu lica sa odgovornošću za upravljanje funkcijom praćenja usaglašenosti navedenom u tački IS.D.OR.200(a)(12).
4. Ukoliko organizacija deli organizacione strukture, politike, procese i procedure bezbednosti informacija sa drugim organizacijama ili sa oblastima sopstvene organizacije koje nisu deo odobrenja ili deklaracije, odgovorni rukovodilac ili, u slučaju projektnih organizacija, rukovodilac projektne organizacije, može delegirati svoje aktivnosti zajedničkom odgovornom licu.

U takvom slučaju, uspostavljaju se mere koordinacije između odgovornog rukovodioca organizacije ili, u slučaju projektantskih organizacija, rukovodioca projektantske organizacije i zajedničkog odgovornog lica kako bi se osigurala adekvatna integracija upravljanja bezbednošću informacija unutar organizacije.

1. Odgovorni rukovodilac ili rukovodilac projektantske organizacije, ili zajedničko odgovorno lice navedeno u tački (d), ima korporativno ovlašćenje da uspostavi i održava organizacione strukture, politike, procese i procedure neophodne za sprovođenje tačke IS.D.OR.200.
2. Organizacija mora imati uspostavljen proces kojim se osigurava da ima dovoljno angažovanog osoblja za obavljanje aktivnosti obuhvaćenih ovim Aneksom.
3. Organizacija mora imati uspostavljen proces kojim se osigurava da osoblje navedeno u tački (f) ima potrebnu kompetentnost za obavljanje svojih zadataka.
4. Organizacija mora imati uspostavljen proces kojim se osigurava da osoblje potvrđuje odgovornosti povezane sa dodeljenim ulogama i zadacima.
5. Organizacija je dužna da obezbedi da se identitet i pouzdanost osoblja koje ima pristup informacionim sistemima i podacima koji podležu zahtevima ove uredbe na odgovarajući način utvrde.

**IS.D.OR.245 Vođenje evidencije**

1. Organizacija mora da vodi evidenciju o svojim aktivnostima upravljanja bezbednošću informacija
   1. Organizacija mora da obezbedi da se sledeći zapisi arhiviraju i da se mogu pratiti:
      1. svako dobijeno odobrenje i svaka povezana procena rizika za bezbednost informacija u skladu sa tačkom IS.D. OR.200(e);
      2. ugovori za aktivnosti navedene u tački IS.D.OR.200(a)(9);
      3. evidencija ključnih procesa navedenih u tački IS.D.OR.200(d);
      4. evidenciju o rizicima identifikovanim u proceni rizika, navedenoj u tački IS.D.OR.205, zajedno sa povezanim merama za tretman rizika navedenim u tački IS.D.OR.210;
      5. evidencija incidenata i ranjivosti u vezi sa informacionom bezbednošću prijavljenih u skladu sa šemama izveštavanja navedenim u tačkama IS.D.OR.215 i IS.D.OR.230;
      6. zapise o onim događajima u vezi sa informacionom bezbednošću koje je možda potrebno ponovo proceniti kako bi se otkrili neotkriveni incidenti ili ranjivosti u vezi sa informacionom bezbednošću.
   2. Evidencija navedena u tački (1)(i) čuva se najmanje 5 godina nakon što odobrenje prestane da važi.
   3. Evidencija navedena u tački (1)(ii) čuva se najmanje 5 godina nakon što je ugovor izmenjen ili raskinut.
   4. Evidencija navedena u tački (1)(iii), (iv) i (v) čuva se najmanje 5 godina.
   5. Evidencije navedene u tački (1)(vi) čuvaju se dok se ti događaji u vezi sa bezbednošću informacija ponovo ne procene u skladu sa periodom definisanim u postupku koji je utvrdila organizacija.
2. Organizacija mora da vodi evidenciju o kvalifikacijama i iskustvu svog osoblja koje je uključeno u aktivnosti upravljanja bezbednošću informacija
   1. Evidencija o kvalifikacijama i iskustvu osoblja čuva se sve dok osoba radi za organizaciju, i najmanje 3 godine nakon što osoba napusti organizaciju.
   2. Članovima osoblja će se, na njihov zahtev, omogućiti pristup njihovim ličnim evidencijama. Pored toga, na njihov zahtev, organizacija će im dostaviti kopiju njihovih individualnih evidencija o napuštanju organizacije.
3. Format evidencija biće preciziran u procedurama za organizuje:.
4. Evidencije se čuvaju na način koji obezbeđuje zaštitu od oštećenja, izmene i krađe, a informacije se identifikuju, kada je to potrebno, u skladu sa njihovim nivoom klasifikacije bezbednosti. Organizacija mora da obezbedi da se evidencije čuvaju korišćenjem sredstava koja obezbeđuju integritet, autentičnost i ovlašćeni pristup.

**IS.D.OR.250 Priručnik za upravljanje bezbednošću informacija (PUBI)**

1. Organizacija mora nadležnom organu staviti na raspolaganje priručnik za upravljanje bezbednošću informacija (PUBI) i, gde je to primenljivo, sve odgovarajuće priručnike i procedure na koje se poziva, koji sadrže:
   1. izjavu koju je potpisao odgovorni rukovodilac ili, u slučaju projektantskih organizacija, rukovodilac projektantske organizacije, kojom se potvrđuje da će organizacija u svakom trenutku raditi u skladu sa ovim Aneksom i sa PUBI-om. Ako odgovorni rukovodilac ili, u slučaju projektantskih organizacija, rukovodilac projektantske organizacije, nije glavni izvršni direktor (CEO) organizacije, onda taj generalni direktor potpisuje izjavu;
   2. titula(e), ime(na), dužnosti, odgovornosti, zaduženja i ovlašćenja lica ili lica navedenih u tački IS.D.OR.240(b) i (c);
   3. titula, ime, dužnosti, odgovornosti, zaduženja i ovlašćenja zajedničkog odgovornog lica navedenog u tački IS.D.OR.240(d), ako je primenljivo;
   4. politika bezbednosti informacija organizacije kako je navedeno u tački IS.D.OR.200(a)(1);
   5. opšti opis broja i kategorija osoblja i sistema koji je na snazi za planiranje raspoloživosti osoblja kako je propisano tačkom IS.D.OR.240;
   6. titula(e), ime(na), dužnosti, odgovornosti, zaduženja i ovlašćenja ključnih lica odgovornih za sprovođenje tačke IS.D.OR.200, uključujući lice ili lica odgovorna za funkciju praćenja usaglašenosti navedenu u tački IS.D.OR.200(a)(12);
   7. organizaciona šema koja prikazuje povezane lance odgovornosti i obaveza za lica navedena u tačkama (2) i (6);
   8. opis interne šeme izveštavanja navedene u tački IS.D.OR.215;
   9. procedure koje određuju kako organizacija obezbeđuje usklađenost sa ovim Delom, a posebno:
      1. tačka dokumentacije IS.D.OR.200(c);
      2. procedure koje definišu kako organizacija kontroliše sve ugovorene aktivnosti navedene u tački IS.D. OR.200(a)(9);
      3. postupak izmene PUBI-a definisan u tački (c);
   10. detalje o trenutno odobrenim alternativnim načinima usaglašenosti.
2. Prvo izdanje PUBI-a mora biti odobreno, a nadležni organ mora da zadrži kopiju. ISMM će se menjati po potrebi kako bi ostao ažuran opis ISMM-a organizacije. Kopija svih izmena PUBI-a mora se dostaviti nadležnom organu.
3. Izmene PUBI-a moraju se upravljati postupkom koji je utvrdila organizacija. Sve izmene koje nisu obuhvaćene ovim postupkom i sve izmene koje se odnose na izmene navedene u tački IS.D. OR.255(b), mora biti odobren od strane nadležnog organa.
4. Organizacija može integrisati PUBI sa drugim priručnicima ili uputstvima za upravljanje koje poseduje, pod uslovom da postoji jasna unakrsna referenca koja pokazuje koji delovi priručnika ili uputstva za upravljanje odgovaraju različitim zahtevima sadržanim u ovom aneksu.

**IS.D.OR.255 Promene sistema upravljanja bezbednošću informacija**

1. Promene SUBI-a mogu se upravljati i o njima se može obavestiti nadležni organ postupkom koji je razvila organizacija. Ovaj postupak odobriće nadležni organ.
2. U vezi sa promenama SUBI-a koje nisu obuhvaćene postupkom navedenim u tački (a), organizacija mora da podnese zahtev i dobije odobrenje koje izdaje nadležni organ.

U vezi sa ovim promenama:

* 1. aplikacija se podnosi pre nego što dođe do takve promene kako bi se omogućilo nadležnom organu da utvrdi kontinuiranu usklađenost sa ovom Uredbom i da izmeni, ako je potrebno, sertifikat organizacije za obuku i propratne uslove odobrenja koji su priloženi uz;
  2. organizacija je dužna da nadležnom organu stavi na raspolaganje sve informacije koje zahteva za procenu promene;
  3. promena će biti sprovedena tek nakon što nadležni organ dobije formalnu saglasnost;
  4. organizacija funkcioniše pod uslovima koje propiše nadležni organ za vreme implementacije takvih promena.

**IS.D.OR.260 Kontinuirano poboljšanje**

1. Organizacija mora da proceni, koristeći odgovarajuće indikatore učinka, efikasnost i zrelost SUBI-a. Ta procena se sprovodi na kalendarskoj osnovi koju je unapred definisala organizacija ili nakon incidenta u vezi sa informacionom bezbednošću.
2. Ako se nakon procene sprovedene u skladu sa tačkom (a) otkriju nedostaci, organizacija preduzima neophodne mere za poboljšanje kako bi osigurala da SUBI i dalje ispunjava važeće zahteve i održava rizike bezbednosti informacija na prihvatljivom nivou. Pored toga, organizacija će ponovo proceniti one elemente SUBI-a na koje utiču usvojene mere.