II

(Icke-lagstiftningsakter)

FÖRORDNINGAR

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2023/203

av den 27 oktober 2022

om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2018/1139 vad gäller krav för hantering av informationssäkerhetsrisker med potentiell inverkan på flygsäkerheten för organisationer som omfattas av kommissionens förordningar (EU) nr 1321/2014, (EU) nr 965/2012, (EU) nr 1178/2011, (EU) 2015/340, kommissionens genomförandeförordningar (EU) 2017/373 och (EU) 2021/664, och för behöriga myndigheter som omfattas av kommissionens förordningar (EU) nr 748/2012, (EU) nr 1321/2014, (EU) nr 965/2012, (EU) nr 1178/2011, (EU) 2015/340 och (EU) nr 139/2014, kommissionens genomförandeförordningar (EU) 2017/373 och (EU) 2021/664 och om ändring av kommissionens förordningar (EU) nr 1178/2011, (EU) nr 748/2012, (EU) nr 965/2012, (EU) nr 139/2014, (EU) nr 1321/2014, (EU) 2015/340, och kommissionens genomförandeförordningar (EU) 2017/373 och (EU) 2021/664

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2018/1139 av den 4 juli 2018 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 2111/2005, (EG) nr 1008/2008, (EU) nr 996/2010, (EU) nr 376/2014 och direktiv 2014/30/EU och 2014/53/EU, samt om upphävande av Europaparlamentets och rådets förordningar (EG) nr 552/2004 och (EG) nr 216/2008 och rådets förordning (EEG) nr 3922/91 [1], särskilt artiklarna 17.1 b, 27.1 a, 31.1 b, 43.1 b, 53.1 a och 62.15 c, och

av följande skäl:

(1) I enlighet med de grundläggande kraven i punkt 3.1 b i bilaga II till förordning (EU) 2018/1139 ska organisationer som svarar för fortsatt luftvärdighet införa och upprätthålla ett ledningssystem för att hantera säkerhetsrisker.

(2) I enlighet med de grundläggande kraven i punkterna 3.3 b och 5 b i bilaga IV till förordning (EU) 2018/1139 ska dessutom utbildningsorganisationer för piloter och kabinbesättningar samt flygmedicinska centrum för flygande personal och operatörer av utbildningshjälpmedel för flygsimulering införa och upprätthålla ett ledningssystem för att hantera säkerhetsrisker.

(3) I enlighet med de grundläggande kraven i punkt 8.1 c i bilaga V till förordning (EU) 2018/1139 ska även luftfartygsoperatörer införa och upprätthålla ett ledningssystem för att hantera säkerhetsrisker.

(4) I enlighet med de grundläggande kraven i punkt 5.1 c och 5.4 b i bilaga VIII till förordning (EU) 2018/1139 ska dessutom leverantörer av flygledningss- och flygtrafiktjänster, leverantörer av U-space-tjänster och leverantörer av gemensamma informationstjänster samt utbildningsorganisationer och flygmedicinska centrum för flygledare införa och upprätthålla ett ledningssystem för att hantera säkerhetsrisker.

[1] EUT L 212, 22.8.2018, s. 1.

(5) Dessa säkerhetsrisker kan härröra från olika källor, såsom konstruktions- och underhållsbrister, aspekter som rör mänskliga prestationer, miljöhot och informationssäkerhetshot. De ledningssystem som införs av Europeiska unionens byrå för luftfartssäkerhet (*byrån*) och de nationella behöriga myndigheter och organisationer som avses i skälen ovan bör därför inte bara beakta säkerhetsrisker som härrör från slumpmässiga händelser, utan även säkerhetsrisker som härrör från informationssäkerhetshot där befintliga brister kan utnyttjas av personer med ont uppsåt. Dessa informationssäkerhetsrisker ökar ständigt inom den civila luftfarten, då de nuvarande informationssystemen blir alltmer sammankopplade och i allt högre grad blir måltavlor för illvilliga aktörer.

(6) De risker som är förknippade med dessa informationssystem är inte begränsade till eventuella cyberangrepp, utan omfattar även hot som kan påverka processer och förfaranden samt människors prestationer.

(7) Ett betydande antal organisationer använder redan internationella standarder, såsom ISO 27001, för att hantera säkerheten för digital information och digitala data. Dessa standarder kanske inte fullt ut tar hänsyn till den civila luftfartens alla särdrag. Därför är det lämpligt att fastställa krav för hanteringen av informationssäkerhetsrisker med en potentiell inverkan på flygsäkerheten.

(8) Det är viktigt att dessa krav omfattar alla luftfartsområden och deras gränssnitt, eftersom luftfarten är ett i hög grad sammanlänkat system av system. De bör därför tillämpas på alla organisationer och behöriga myndigheter som omfattas av kommissionens förordningar (EU) nr 748/2012 ([2]), (EU) nr 1321/2014 ([3]), (EU) nr 965/2012 ([4]), (EU) nr 1178/2011 ([5]), (EU) 2015/340 ([6]), (EU) nr 139/2014 ([7]) och kommissionens genomförandeförordning (EU) 2021/664 ([8]), även de organisationer och behöriga myndigheter som redan är skyldiga att ha ett ledningssystem i enlighet med unionens befintliga flygsäkerhetslagstiftning. Vissa organisationer bör dock undantas från denna förordnings tillämpningsområde för att säkerställa lämplig proportionalitet mot de lägre informationssäkerhetsrisker som de utgör för luftfartssystemet.

(9) De krav som fastställs i denna förordning bör säkerställa ett konsekvent genomförande inom alla luftfartsområden, samtidigt som de skapar en minimal inverkan på den unionslagstiftning om flygsäkerhet som redan är tillämplig på dessa områden.

([2]) Kommissionens förordning (EU) nr 748/2012 av den 3 augusti 2012 om fastställande av tillämpningsföreskrifter för luftvärdighets- och miljöcertifiering av luftfartyg och tillhörande produkter, delar och anordningar samt för certifiering av konstruktions- och tillverkningsorganisationer (EUT L 224, 21.8.2012, s. 1).

([3]) Kommissionens förordning (EU) nr 1321/2014 av den 26 november 2014 om fortsatt luftvärdighet för luftfartyg och luftfartygsprodukter, delar och anordningar och om godkännande av organisationer och personal som arbetar med dessa arbetsuppgifter (omarbetning) (EUT L 362, 17.12.2014, s. 1).

([4]) Kommissionens förordning (EU) nr 965/2012 av den 5 oktober 2012 om tekniska krav och administrativa förfaranden i samband med flygdrift enligt Europaparlamentets och rådets förordning (EG) nr 216/2008 (EUT L 296, 25.10.2012, s. 1).

([5]) Kommissionens förordning (EU) nr 1178/2011 av den 3 november 2011 om tekniska krav och administrativa förfaranden avseende flygande personal inom den civila luftfarten i enlighet med Europaparlamentets och rådets förordning (EG) nr 216/2008 (EUT L 311, 25.11.2011, s. 1).

([6]) Kommissionens förordning (EU) 2015/340 av den 20 februari 2015 om tekniska krav och administrativa förfaranden avseende flygledarcertifikat samt andra certifikat och intyg enligt Europaparlamentets och rådets förordning (EG) nr 216/2008, ändring av kommissionens genomförandeförordning (EU) nr 923/2012 och upphävande av kommissionens förordning (EU) nr 805/2011 (EUT L 63, 6.3.2015, s. 1).

([7]) Kommissionens förordning (EU) nr 139/2014 av den 12 februari 2014 om krav och administrativa rutiner för flygplatser enligt Europaparlamentets och rådets förordning (EG) nr 216/2008 (EUT L 44, 14.2.2014, s. 1).

([8]) Kommissionens genomförandeförordning (EU) 2021/664 av den 22 april 2021 om ett regelverk för U-space (EUT L 139, 23.4.2021, s. 161).

(10) De krav som fastställs i denna förordning bör inte påverka de krav på informationssäkerhet och cybersäkerhet som anges i punkt 1.7 i bilagan till kommissionens genomförandeförordning (EU) 2015/1998 ([9]) och i artikel 14 i Europaparlamentets och rådets direktiv (EU) 2016/1148 ([10]).

(11) De säkerhetskrav som fastställs i artiklarna 33–43 i avdelning V ”Programmets säkerhet” i Europaparlamentets och rådets förordning (EU) 2021/696 ([11]) anses vara likvärdiga med kraven i den här förordningen, med undantag för kraven i punkt IS.I.OR.230 i bilaga II till den här förordningen vilka bör uppfyllas.

(12) För att skapa rättssäkerhet bör tolkningen av begreppet *informationssäkerhet* enligt definitionen i den här förordningen, som återspeglar dess gemensamma användning inom den civila luftfarten på global nivå, anses vara förenlig med begreppet *säkerhet i nätverks- och informationssystem* enligt definitionen i artikel 4.2 i direktiv (EU) 2016/1148. Den definition av *informationssäkerhet* som används i den här förordningen bör inte tolkas som en avvikelse från den definition av *säkerhet i nätverks- och informationssystem* som fastställs i direktiv (EU) 2016/1148.

(13) När organisationer som omfattas av denna förordning redan omfattas av säkerhetskrav som följer av de unionsakter som avses i skälen 10 och 11 och som till sin verkan är likvärdiga med bestämmelserna i denna förordning bör uppfyllelse av dessa säkerhetskrav, för att undvika dubblering av rättsliga krav, anses utgöra uppfyllelse av de krav som fastställs i denna förordning.

(14) Organisationer som omfattas av denna förordning och som redan omfattas av säkerhetskrav som följer av kommissionens genomförandeförordning (EU) 2015/1998 eller förordning (EU) 2021/696, eller båda, bör också uppfylla kraven i bilaga II (Del IS.I.OR.230 ”Externt rapporteringssystem för informationssäkerhet”) till denna förordning eftersom ingen av dessa förordningar innehåller några bestämmelser om extern rapportering av informationssäkerhetsincidenter.

(15) För fullständighetens skull bör förordningarna (EU) nr 1178/2011, (EU) nr 748/2012, (EU) nr 965/2012, (EU) nr 139/2014, (EU) nr 1321/2014, (EU) 2015/340 och genomförandeförordningarna (EU) 2017/373 ([12]) och (EU) 2021/664 ändras så att de krav på system för hantering av informationssäkerhet som föreskrivs i denna förordning införs, tillsammans med de ledningssystem som fastställs däri, och så att de behöriga myndigheternas krav fastställs beträffande tillsynen av de organisationer som genomför ovannämnda krav på system för hantering av informationssäkerhet.

(16) För att ge organisationer tillräckligt med tid för att säkerställa efterlevnaden av de nya reglerna och förfarandena bör denna förordning gälla i tre år efter dess ikraftträdande, med undantag för leverantören av flygtrafiktjänster för Egnos (*European Geostationary Navigation Overlay Service*) enligt definitionen i genomförandeförordning (EU) 2017/373, där den på grund av den pågående säkerhetsackrediteringen av Egnossystemet och Egnostjänsterna i enlighet med förordning (EU) 2021/696 bör bli tillämplig den 1 januari 2026.

(17) De krav som fastställs i denna förordning grundar sig på yttrande nr 03/2021 ([13]) som utfärdats av byrån i enlighet med artikel 75.2 b och c och artikel 76.1 i förordning (EU) 2018/1139.

([9]) Kommissionens genomförandeförordning (EU) 2015/1998 av den 5 november 2015 om detaljerade bestämmelser för genomförande av de gemensamma grundläggande standarderna avseende luftfartsskydd (EUT L 299, 14.11.2015, s. 1).

([10]) Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).

([11]) Europaparlamentets och rådets förordning (EU) 2021/696 av den 28 april 2021 om inrättande av unionens rymdprogram och Europeiska unionens rymdprogrambyrå och om upphävande av förordningarna (EU) nr 912/2010, (EU) nr 1285/2013 och (EU) nr 377/2014 och beslut nr 541/2014/EU (EUT L 170, 12.5.2021, s. 69).

([12]) Kommissionens genomförandeförordning (EU) 2017/373 av den 1 mars 2017 om gemensamma krav för leverantörer av flygledningstjänst/flygtrafiktjänster och övriga nätverksfunktioner för flygledningstjänst, om tillsyn över dessa leverantörer samt om upphävande av förordning (EG) nr 482/2008, genomförandeförordningarna (EU) nr 1034/2011, (EU) nr 1035/2011 och (EU) 2016/1377 och ändring av förordning (EU) nr 677/2011 (EUT L 62, 8.3.2017, s. 1).

([13]) https://www.easa.europa.eu/en/document-library/opinions/opinion-032021

(18) De krav som fastställs i denna förordning är förenliga med yttrandet från den kommitté för tillämpning av gemensamma säkerhetsbestämmelser på det civila luftfartsområdet som inrättats genom artikel 127 i förordning (EU) 2018/1139.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Innehåll

I denna förordning fastställs de krav som organisationer och behöriga myndigheter ska uppfylla för att

a) identifiera och hantera informationssäkerhetsrisker med potentiell inverkan på flygsäkerheten vilka skulle kunna påverka informations- och kommunikationstekniksystem och data som används för civil luftfart,

b) upptäcka informationssäkerhetshändelser och identifiera de händelser som anses utgöra informationssäkerhetsincidenter med potentiell inverkan på flygsäkerheten,

c) hantera dessa informationssäkerhetsincidenter, även när det gäller återställning efter dem.

Artikel 2

Tillämpningsområde

1. Denna förordning är tillämplig på följande organisationer:

a) Underhållsorganisationer som omfattas av avsnitt A i bilaga II (Del-145) till förordning (EU) nr 1321/2014, utom de som enbart bedriver underhåll av luftfartyg i enlighet med bilaga Vb (Del-ML) till förordning (EU) nr 1321/2014.

b) Organisationer som svarar för fortsatt luftvärdighet vilka omfattas av avsnitt A i bilaga Vc (Del-CAMO) till förordning (EU) nr 1321/2014, utom de som enbart ägnar sig åt arbete för fortsatt luftvärdighet för luftfartyg i enlighet med bilaga Vb (Del-ML) till förordning (EU) nr 1321/2014.

c) Luftfartygsoperatörer som omfattas av bilaga III (Del-ORO) till förordning (EU) nr 965/2012, utom de som enbart ägnar sig åt driften av något av följande:

i) Ett ELA2-luftfartyg enligt definitionen i artikel 1.2 j i förordning (EU) nr 748/2012.

ii) Enmotoriga propellerdrivna flygplan som har en maximal operativ kabinkonfiguration för befordran av högst fem passagerare och som inte är klassificerade som komplexa motordrivna luftfartyg, när de startar och landar på samma flygplats eller utelandningsplats, enligt visuellflygregler under dager.

iii) Enmotoriga helikoptrar som har en maximal operativ kabinkonfiguration för befordran av högst fem passagerare och som inte är klassificerade som komplexa motordrivna luftfartyg, när de startar och landar på samma flygplats eller utelandningsplats, enligt visuellflygregler under dager.

d) Godkända utbildningsorganisationer som omfattas av bilaga VII (Del-ORA) till förordning (EU) nr 1178/2011, utom de som enbart tillhandahåller utbildning avseende ELA2-luftfartyg enligt definitionen i artikel 1.2 j i förordning (EU) nr 748/2012, eller som enbart tillhandahåller teoretisk utbildning.

e) Flygmedicinska centrum för flygande personal vilka omfattas av bilaga VII (Del-ORA) till förordning (EU) nr 1178/2011.

f) Operatörer av utbildningshjälpmedel för flygsimulering vilka omfattas av bilaga VII (Del-ORA) till förordning (EU) nr 1178/2011, utom de som enbart arbetar med driften av utbildningshjälpmedel för flygsimulering avseende ELA2-luftfartyg enligt definitionen i artikel 1.2 j i förordning (EU) nr 748/2012.

g) Organisationer som bedriver flygledarutbildning samt flygmedicinska centrum för flygledare som omfattas av bilaga III (Del-ATCO.OR) till förordning (EU) 2015/340.

h) Organisationer som omfattas av bilaga III (Del-ATM/ANS.OR) till genomförandeförordning (EU) 2017/373, utom följande tjänsteleverantörer:

i) Leverantörer av flygtrafiktjänster som innehar ett begränsat certifikat i enlighet med punkt ATM/ANS.OR.A.010 i den bilagan.

ii) Leverantörer av flyginformationstjänst som lämnar in en försäkran om sin verksamhet i enlighet med punkt ATM/ANS.OR.A.015 i den bilagan.

i) Leverantörer av U-space-tjänster och leverantörer av gemensamma informationstjänster som omfattas av genomförandeförordning (EU) 2021/664.

2. Denna förordning är tillämplig på de behöriga myndigheter, inklusive Europeiska unionens byrå för luftfartssäkerhet (*byrån*), som avses i artikel 6 i denna förordning och i artikel 5 i kommissionens delegerade förordning (EU) 2022/1645 ([14]).

3. Denna förordning är också tillämplig på den behöriga myndighet som ansvarar för utfärdande, förlängning, ändring, upphävande eller återkallande av certifikat för luftfartygsunderhåll i enlighet med bilaga III (Del-66) till förordning (EU) nr 1321/2014.

4. Denna förordning påverkar inte de krav på informationssäkerhet och cybersäkerhet som anges i punkt 1.7 i bilagan till genomförandeförordning (EU) 2015/1998 och i artikel 14 i direktiv (EU) 2016/1148.

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

1. *informationssäkerhet*: bevarande av nätverks- och informationssystemens konfidentialitet, integritet, autenticitet och tillgänglighet.

2. *informationssäkerhetshändelse*: ett konstaterat system-, tjänste- eller nätverkstillstånd som tyder på en möjlig överträdelse av informationssäkerhetspolicyn eller fel i informationssäkerhetskontrollerna, eller en tidigare okänd situation som kan vara relevant för informationssäkerhet.

3. *incident*: en händelse med en faktisk negativ inverkan på säkerheten i nätverks- och informationssystem enligt definitionen i artikel 4.7 i direktiv (EU) 2016/1148.

4. *informationssäkerhetsrisk*: risken för organisatorisk civil luftfartsverksamhet, tillgångar, personer och andra organisationer på grund av potentialen för en informationssäkerhetshändelse. Informationssäkerhetsrisker är förknippade med potentialen att hot kommer att utnyttja sårbarheter i en informationstillgång eller en grupp av informationstillgångar.

([14]) Kommissionens delegerade förordning (EU) 2022/1645 av den 14 juli 2022 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2018/1139 vad gäller krav för hantering av informationssäkerhetsrisker med potentiell inverkan på flygsäkerheten för organisationer som omfattas av kommissionens förordningar (EU) nr 748/2012 och (EU) nr 139/2014, och om ändring av kommissionens förordningar (EU) nr 748/2012 och (EU) nr 139/2014 (EUT L 248, 26.9.2022, s. 18).

5. *hot*: en potentiell kränkning av informationssäkerheten som föreligger när det finns en enhet, omständighet, handling eller händelse som skulle kunna orsaka skada.

6. *sårbarhet*: en brist eller svaghet i en tillgång eller ett system, förfaranden, konstruktion, genomförande eller informationssäkerhetsåtgärder som skulle kunna utnyttjas och som leder till en överträdelse eller kränkning av informationssäkerhetspolicyn.

Artikel 4

Krav för organisationer och behöriga myndigheter

1. De organisationer som avses i artikel 2.1 ska uppfylla kraven i bilaga II (Del-IS.I.OR) till denna förordning.

2. De behöriga myndigheter som avses i artikel 2.2 och 2.3 ska uppfylla kraven i bilaga I (Del-IS.AR) till denna förordning.

Artikel 5

Krav som följer av annan unionslagstiftning

1. När en organisation som avses i artikel 2.1 uppfyller sådana säkerhetskrav som fastställts i enlighet med artikel 14 i direktiv (EU) 2016/1148 och som är likvärdiga med kraven i den här förordningen, ska uppfyllelse av dessa säkerhetskrav anses utgöra uppfyllelse av kraven i den här förordningen.

2. När en organisation som avses i artikel 2.1 är en operatör eller en verksamhetsutövare som avses i medlemsstaternas nationella säkerhetsprogram för civil luftfart vilket utarbetats i enlighet med artikel 10 i Europaparlamentets och rådets förordning (EG) nr 300/2008 ([15]), ska cybersäkerhetskraven i punkt 1.7 i bilagan till genomförandeförordning (EU) 2015/1998 anses vara likvärdiga med kraven i den här förordningen, med undantag för kraven i punkt IS.I.OR.230 i bilaga II till den här förordningen vilka ska uppfyllas.

3. När den organisation som avses i artikel 2.1 är den leverantör av flygtrafiktjänster för Egnos (*European Geostationary Navigation Overlay Service*) som avses i förordning (EU) 2021/696, anses säkerhetskraven i artiklarna 33–43 i avdelning V i den förordningen vara likvärdiga med kraven i den här förordningen, med undantag för kraven i punkt IS.I.OR.230 i bilaga II till den här förordningen vilka ska uppfyllas.

4. Kommissionen får, efter samråd med byrån och den samarbetsgrupp som avses i artikel 11 i direktiv (EU) 2016/1148, utfärda riktlinjer för bedömningen av likvärdigheten av de krav som fastställs i denna förordning och i direktiv (EU) 2016/1148.

Artikel 6

Behörig myndighet

1. Utan att det påverkar de arbetsuppgifter som anförtros den styrelse för säkerhetsackreditering som avses i artikel 36 i förordning (EU) 2021/696 ska den myndighet som ansvarar för att certifiera och övervaka efterlevnaden av denna förordning vara

a) den behöriga myndighet som utsetts i enlighet med bilaga II (Del-145) till förordning (EU) nr 1321/2014, när det gäller organisationer som avses i artikel 2.1 a,

b) den behöriga myndighet som utsetts i enlighet med bilaga Vc (Del-CAMO) till förordning (EU) nr 1321/2014, när det gäller organisationer som avses i artikel 2.1 b,

([15]) Europaparlamentets och rådets förordning (EG) nr 300/2008 av den 11 mars 2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002 (EUT L 97, 9.4.2008, s. 72).

c) den behöriga myndighet som utsetts i enlighet med bilaga III (Del-ORO) till förordning (EU) nr 965/2012, när det gäller organisationer som avses i artikel 2.1 c,

d) den behöriga myndighet som utsetts i enlighet med bilaga VII (Del-ORA) till förordning (EU) nr 1178/2011, när det gäller organisationer som avses i artikel 2.1 d–f,

e) den behöriga myndighet som utsetts i enlighet med artikel 6.2 i förordning (EU) 2015/340, när det gäller organisationer som avses i artikel 2.1 g,

f) den behöriga myndighet som utsetts i enlighet med artikel 4.1 i genomförandeförordning (EU) 2017/373, när det gäller organisationer som avses i artikel 2.1 h,

g) den behöriga myndighet som utsetts i enlighet med artikel 14.1 eller 14.2, beroende på vad som är tillämpligt, i genomförandeförordning (EU) 2021/664, när det gäller organisationer som avses i artikel 2.1 i.

2. Medlemsstaterna får för tillämpningen av denna förordning utse en oberoende och autonom enhet som ska fullgöra den roll och det ansvar som tilldelas de behöriga myndigheter som avses i punkt 1. I sådana fall ska samordningsåtgärder fastställas mellan den enheten och de behöriga myndigheter som avses i punkt 1 för att säkerställa en effektiv tillsyn av alla krav som organisationen ska uppfylla.

3. Byrån ska samarbeta i full överensstämmelse med de tillämpliga reglerna om sekretess, skydd av personuppgifter och skydd av säkerhetsskyddsklassificerade uppgifter med Europeiska unionens rymdprogrambyrå (EUSPA) och den styrelse för säkerhetsackreditering som avses i artikel 36 i förordning (EU) 2021/696 för att säkerställa en effektiv tillsyn av de krav som är tillämpliga på leverantörer av flygtrafiktjänster för Egnos.

Artikel 7

Inlämning av relevant information till de behöriga myndigheterna för säkerhet i nätverks- och informationssystem

Behöriga myndigheter enligt denna förordning ska utan onödigt dröjsmål meddela den gemensamma kontaktpunkt som utsetts i enlighet med artikel 8 i direktiv (EU) 2016/1148 all relevant information som ingår i anmälningar som lämnats in i enlighet med punkt IS.I.OR.230 i bilaga II till denna förordning och punkt IS.D.OR.230 i bilaga I till delegerad förordning 2022/1645 av leverantörer av samhällsviktiga tjänster som identifierats i enlighet med artikel 5 i direktiv (EU) 2016/1148.

Artikel 8

Ändring av förordning (EU) nr 1178/2011

Bilagorna VI (Del-ARA) och VII (Del-ORA) till förordning (EU) nr 1178/2011 ska ändras i enlighet med bilaga III till den här förordningen.

Artikel 9

Ändring av förordning (EU) nr 748/2012

Bilaga I (Del-21) till förordning (EU) nr 748/2012 ska ändras i enlighet med bilaga IV till den här förordningen.

Artikel 10

Ändring av förordning (EU) nr 965/2012

Bilagorna II (Del-ARO) och III (Del-ORO) till förordning (EU) nr 965/2012 ska ändras i enlighet med bilaga V till den här förordningen.

Artikel 11

Ändring av förordning (EU) nr 139/2014

Bilaga II (Del-ADR.AR) till förordning (EU) nr 139/2014 ska ändras i enlighet med bilaga VI till den här förordningen.

Artikel 12

Ändring av förordning (EU) nr 1321/2014

Bilagorna II (Del-145), III (Del-66) och Vc (Del-CAMO) till förordning (EU) nr 1321/2014 ska ändras i enlighet med bilaga VII till den här förordningen.

Artikel 13

Ändring av förordning (EU) 2015/340

Bilagorna II (Del-ATCO.AR) och III (Del-ATCO.OR) till förordning (EU) 2015/340 ska ändras i enlighet med bilaga VIII till den här förordningen.

Artikel 14

Ändring av genomförandeförordning (EU) 2017/373

Bilagorna II (Del-ATM/ANS.AR) och III (Del-ATM/ANS.OR) till genomförandeförordning (EU) 2017/373 ska ändras i enlighet med bilaga IX till den här förordningen.

Artikel 15

Ändring av genomförandeförordning (EU) 2021/664

Genomförandeförordning (EU) 2021/664 ska ändras på följande sätt:

1. I artikel 15.1 ska punkt f ersättas med följande:

”f) inför och upprätthåller ett skyddsledningssystem i enlighet med punkt ATM/ANS.OR.D.010 i kapitel D i bilaga III till genomförandeförordning (EU) 2017/373 och ett system för hantering av informationssäkerhet i enlighet med bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203,”.

2. I artikel 18 ska följande punkt läggas till som punkt l:

”l) inrätta, genomföra och upprätthålla ett system för hantering av informationssäkerhet i enlighet med bilaga I (Del-IS.AR) till genomförandeförordning (EU) 2023/203.”.

Artikel 16

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Den ska tillämpas från och med den 22 februari 2026.

När det gäller den leverantör av flygtrafiktjänster för Egnos som omfattas av genomförandeförordning (EU) 2017/373 ska den dock tillämpas från och med den 1 januari 2026.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 27 oktober 2022.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

BILAGA I

INFORMATIONSSÄKERHET – MYNDIGHETSKRAV

[DEL-IS.AR]

IS.AR.100 Tillämpningsområde

I denna del fastställs de verksamhetskrav som ska uppfyllas av de behöriga myndigheter som avses i artikel 2.2 i denna förordning.

De krav som dessa behöriga myndigheter ska uppfylla när den bedriver sin verksamhet för certifiering, tillsyn och kontroll av efterlevnaden finns i de förordningar som avses i artikel 2.1 i denna förordning och i artikel 2 i delegerad förordning (EU) 2022/1645.

IS.AR.200 System för hantering av informationssäkerhet (ISMS)

a) För att uppnå de mål som anges i artikel 1 ska den behöriga myndigheten inrätta, genomföra och upprätthålla ett system för hantering av informationssäkerhet (ISMS) som säkerställer att den behöriga myndigheten

1) inrättar en policy för informationssäkerhet som fastställer den behöriga myndighetens övergripande principer med avseende på informationssäkerhetsriskernas potentiella inverkan på flygsäkerheten,

2) identifierar och ser över informationssäkerhetsrisker i enlighet med punkt IS.AR.205,

3) definierar och genomför åtgärder för hantering av informationssäkerhetsrisker i enlighet med punkt IS.AR.210,

4) definierar och genomför, i enlighet med punkt IS.AR.215, de åtgärder som krävs för att upptäcka informationssäkerhetshändelser, identifierar de händelser som anses vara incidenter med en potentiell inverkan på flygsäkerheten samt hanterar och sköter återställning efter sådana informationssäkerhetsincidenter,

5) uppfyller kraven i punkt IS.AR.220 när den utkontrakterar någon del av den verksamhet som beskrivs i punkt IS.AR.200 till andra organisationer,

6) uppfyller de personalkrav som anges i punkt IS.AR.225,

7) uppfyller de dokumentationskrav som anges i punkt IS.AR.230,

8) övervakar att den egna organisationen uppfyller kraven i denna förordning och ger återkoppling om brister till den person som avses i punkt IS.AR.225 a för att säkerställa ett effektivt genomförande av korrigerande åtgärder,

9) skyddar konfidentialiteten för all information som den behöriga myndigheten innehar och som är kopplad till organisationer som står under dess tillsyn samt information som mottagits genom organisationens externa rapporteringssystem som inrättats i enlighet med punkt IS.I.OR.230 i bilaga II (Del-IS.I.OR) till denna förordning och punkt IS.D.OR.230 i bilagan (Del-IS.D.OR) till delegerad förordning (EU) 2022/1645,

10) underrättar byrån om ändringar som påverkar den behöriga myndighetens förmåga att utföra sina arbetsuppgifter och fullgöra sina skyldigheter enligt denna förordning,

11) definierar och genomför förfaranden för att, när så är lämpligt samt på ett praktiskt sätt och i god tid, utbyta relevant information för att bistå andra behöriga myndigheter och byråer, samt organisationer som omfattas av denna förordning, för att genomföra effektiva bedömningar av säkerhetsrisker kopplade till deras verksamhet.

b) För att kontinuerligt uppfylla de krav som avses i artikel 1 ska den behöriga myndigheten genomföra en kontinuerlig förbättringsprocess i enlighet med punkt IS.AR.235.

c) Den behöriga myndigheten ska dokumentera alla centrala processer, förfaranden, roller och ansvarsområden som krävs för att uppfylla kraven i punkt IS.AR.200 a och inrätta en process för att ändra denna dokumentation.

d) De processer, förfaranden, roller och ansvarsområden som den behöriga myndigheten inrättat för att uppfylla kraven i punkt IS.AR.200 a ska motsvara verksamhetens art och komplexitet, på grundval av en bedömning av de informationssäkerhetsrisker som är förknippade med denna verksamhet, och får integreras i andra befintliga ledningssystem som den behöriga myndigheten redan infört.

IS.AR.205 Bedömning av informationssäkerhetsrisker

a) Den behöriga myndigheten ska identifiera alla delar av den egna organisationen som skulle kunna utsättas för informationssäkerhetsrisker. Detta ska innefatta

1) den behöriga myndighetens verksamhet, anläggningar och resurser samt de tjänster som den behöriga myndigheten driver, tillhandahåller, tar emot eller upprätthåller,

2) den utrustning och information och de system och data som bidrar till att de delar som avses i punkt 1 fungerar.

b) Den behöriga myndigheten ska identifiera de gränssnitt som den egna organisationen har mot andra organisationer och som kan leda till ömsesidig exponering för informationssäkerhetsrisker.

c) När det gäller de delar och gränssnitt som avses i punkterna a och b ska den behöriga myndigheten identifiera de informationssäkerhetsrisker som kan ha en potentiell inverkan på flygsäkerheten.

För varje identifierad risk ska den behöriga myndigheten

1) tilldela en risknivå enligt en fördefinierad klassificering som fastställts av den behöriga myndigheten,

2) associera varje risk och dess nivå med motsvarande del eller gränssnitt som identifierats i enlighet med punkterna a och b.

Den fördefinierade klassificering som avses i punkt 1 ska ta hänsyn till risken för att hotscenariot inträffar och hur allvarliga konsekvenser det skulle få för säkerheten. Genom denna klassificering, och med beaktande av huruvida den behöriga myndigheten har en strukturerad och repeterbar riskhanteringsprocess för verksamheten, ska den behöriga myndigheten kunna fastställa om risken är acceptabel eller behöver hanteras i enlighet med punkt IS.AR.210.

För att underlätta riskbedömningarnas ömsesidiga jämförbarhet ska tilldelningen av risknivå enligt punkt 1 ta hänsyn till relevant information som erhållits i samordning med de organisationer som avses i punkt b.

d) Den behöriga myndigheten ska se över och uppdatera den riskbedömning som utförts i enlighet med punkterna a, b och c i något av följande fall:

1) Det sker en förändring i de delar som omfattas av informationssäkerhetsrisker.

2) Det sker en förändring i gränssnitten mellan den behöriga myndighetens organisation och andra organisationer, eller i de risker som meddelats av de andra organisationerna.

3) Det sker en förändring i den information eller kunskap som används för att identifiera, analysera och klassificera risker.

4) Lärdom dras av analysen av informationssäkerhetsincidenter.

IS.AR.210 Hantering av informationssäkerhetsrisker

a) Den behöriga myndigheten ska utarbeta åtgärder för att hantera oacceptabla risker som identifierats i enlighet med punkt IS.AR.205 samt genomföra dem i rätt tid och kontrollera att de fortfarande är effektiva. Dessa åtgärder ska göra det möjligt för den behöriga myndigheten att

1) kontrollera de omständigheter som bidrar till att hotscenariot faktiskt inträffar,

2) minska konsekvenserna för flygsäkerheten i samband med att hotscenariot förverkligas,

3) undvika riskerna.

Dessa åtgärder får inte medföra några nya potentiella oacceptabla risker för flygsäkerheten.

b) Den person som avses i punkt IS.AR.225 a och annan berörd personal vid den behöriga myndigheten ska informeras om resultatet av den riskbedömning som utförts i enlighet med punkt IS.AR.205, motsvarande hotscenarier och de åtgärder som ska vidtas.

Den behöriga myndigheten ska också informera organisationer mot vilka den har ett gränssnitt i enlighet med punkt IS.AR.205 b om eventuella risker som är gemensamma för den behöriga myndigheten och organisationen.

IS.AR.215 Informationssäkerhetsincidenter – upptäckt, hantering och återställning

a) På grundval av resultatet av den riskbedömning som utförts i enlighet med punkt IS.AR.205 och resultatet av den riskhantering som utförts i enlighet med punkt IS.AR.210 ska den behöriga myndigheten vidta åtgärder för att upptäcka händelser som visar att oacceptabla risker potentiellt kan förverkligas och som kan ha en potentiell inverkan på flygsäkerheten. Dessa upptäcktsåtgärder ska göra det möjligt för den behöriga myndigheten att

1) identifiera avvikelser från fördefinierade utgångsvärden för funktionsprestanda,

2) utlösa varningar för att aktivera lämpliga reaktionsåtgärder, vid eventuella avvikelser.

b) Den behöriga myndigheten ska vidta åtgärder för att reagera på alla händelseförhållanden som identifierats i enlighet med punkt a och som kan utvecklas eller har utvecklats till en informationssäkerhetsincident. Dessa reaktionsåtgärder ska göra det möjligt för den behöriga myndigheten att

1) inleda den egna organisationens reaktion på de varningar som avses i punkt a.2 genom att aktivera fördefinierade resurser och åtgärder,

2) begränsa spridningen av en attack och undvika att ett hotscenario förverkligas fullt ut,

3) kontrollera felläget för de berörda delar som anges i punkt IS.AR.205 a.

c) Den behöriga myndigheten ska vidta åtgärder som syftar till återställning efter informationssäkerhetsincidenter, inbegripet nödåtgärder om så behövs. Dessa återställningsåtgärder ska göra det möjligt för den behöriga myndigheten att

1) eliminera det förhållande som orsakade incidenten eller begränsa det till en acceptabel nivå,

2) återställa ett säkert tillstånd för de berörda delar som anges i punkt IS.AR.205 a inom en återställningstid som tidigare fastställts av den egna organisationen.

IS.AR.220 Utkontraktering av verksamhet som rör hantering av informationssäkerhet

Vid utkontraktering av någon del av den verksamhet som avses i punkt IS.AR.200 till andra organisationer ska den behöriga myndigheten säkerställa att den utkontrakterade verksamheten uppfyller kraven i denna förordning och att underleverantören arbetar under dess tillsyn. Den behöriga myndigheten ska säkerställa att de risker som är förenade med den utkontrakterade verksamheten hanteras på lämpligt sätt.

IS.AR.225 Personalkrav

Den behöriga myndigheten ska uppfylla följande krav:

a) Den behöriga myndigheten ska ha en person som är bemyndigad att upprätta och upprätthålla de organisatoriska strukturer, policyer, processer och förfaranden som krävs för att genomföra denna förordning.

Denna person ska

1) vara bemyndigad att till fullo utnyttja de resurser som krävs för att den behöriga myndigheten ska kunna utföra alla de uppgifter som krävs enligt denna förordning,

2) kunna delegera befogenheter när så krävs för att utföra de tilldelade uppgifterna.

b) Den behöriga myndigheten ska ha en process för att säkerställa att den har tillräckligt med personal i tjänst för att kunna utföra den verksamhet som omfattas av denna bilaga.

c) Den behöriga myndigheten ska ha en process för att säkerställa att den personal som avses i punkt b har den kompetens som krävs för att utföra uppgifterna.

d) Den behöriga myndigheten ska ha en process för att säkerställa att personalen är medveten om det ansvar som är förenat med de tilldelade rollerna och uppgifterna.

e) Den behöriga myndigheten ska säkerställa att identiteten på och tillförlitligheten hos den personal som har åtkomst till informationssystem och data som omfattas av kraven i denna förordning fastställs på lämpligt sätt.

IS.AR.230 Dokumentation

a) Den behöriga myndigheten ska dokumentera sin verksamhet för hantering av informationssäkerhet.

1) Den behöriga myndigheten ska säkerställa att följande dokumentation arkiveras och kan spåras:

i) Kontrakt för verksamhet som avses i punkt IS.AR.200 a.5.

ii) Dokumentation av de centrala processer som avses i punkt IS.AR.200 d.

iii) Dokumentation av de risker som identifierats i den riskbedömning som avses i punkt IS.AR.205 tillsammans med de tillhörande riskhanteringsåtgärder som avses i punkt IS.AR.210.

iv) Dokumentation av informationssäkerhetshändelser som kan behöva omprövas för att avslöja oupptäckta informationssäkerhetsincidenter eller sårbarheter.

2) Den dokumentation som avses i punkt 1 i ska bevaras i minst fem år efter det att kontraktet har ändrats eller sagts upp.

3) Den dokumentation som avses i punkt 1 ii och iii ska bevaras i minst fem år.

4) Den dokumentation som avses i punkt 1 iv ska bevaras till dess att dessa informationssäkerhetshändelser har omprövats i enlighet med en periodicitet som anges i ett förfarande som fastställts av den behöriga myndigheten.

b) Den behöriga myndigheten ska ha dokumentation över kvalifikationer och erfarenhet när det gäller den egna personalen som arbetar med hantering av informationssäkerhet.

1) Dokumentationen av personalens kvalifikationer och erfarenhet ska bevaras så länge personen arbetar för den behöriga myndigheten och i minst tre år efter det att personen har lämnat den behöriga myndigheten.

2) Anställda ska på egen begäran få tillgång till den dokumentation som gäller dem. På deras begäran ska den behöriga myndigheten också ge dem en kopia av den dokumentation som gäller dem när de lämnar den behöriga myndigheten.

c) Formatet för dokumentationen ska anges i den behöriga myndighetens förfaranden.

d) Dokumentationen ska lagras på ett sätt som säkerställer skydd från skada, ändring och stöld, vid behov med uppgift om informationens säkerhetsskyddsklassificeringsnivå. Den behöriga myndigheten ska säkerställa att dokumentationen lagras på ett sätt som säkerställer integritet, autenticitet och behörig åtkomst.

IS.AR.235 Löpande förbättring

a) Den behöriga myndigheten ska med hjälp av lämpliga resultatindikatorer bedöma effektiviteten och mognadsgraden hos dess egna ISMS. Bedömningen ska utföras enligt en tidsplan som fastställts på förhand av den behöriga myndigheten eller till följd av en informationssäkerhetsincident.

b) Om brister upptäcks till följd av den bedömning som utförts i enlighet med punkt a ska den behöriga myndigheten vidta nödvändiga förbättringsåtgärder för att säkerställa att ISMS fortsätter att uppfylla de tillämpliga kraven och upprätthåller en acceptabel nivå för informationssäkerhetsriskerna. Dessutom ska den behöriga myndigheten göra en ny bedömning av de delar av ISMS som påverkas av de antagna åtgärderna.

BILAGA II

INFORMATIONSSÄKERHET – ORGANISATIONSKRAV

[DEL-IS.I.OR]

IS.I.OR.100 Tillämpningsområde

I denna del fastställs de krav som ska uppfyllas av de organisationer som avses i artikel 2.1 i denna förordning.

IS.I.OR.200 System för hantering av informationssäkerhet (ISMS)

a) För att uppnå de mål som anges i artikel 1 ska organisationen inrätta, genomföra och upprätthålla ett system för hantering av informationssäkerhet (ISMS) som säkerställer att organisationen

1) inrättar en policy för informationssäkerhet som fastställer organisationens övergripande principer med avseende på informationssäkerhetsriskernas potentiella inverkan på flygsäkerheten,

2) identifierar och ser över informationssäkerhetsrisker i enlighet med punkt IS.I.OR.205,

3) definierar och genomför åtgärder för hantering av informationssäkerhetsrisker i enlighet med punkt IS.I.OR.210,

4) genomför ett internt rapporteringssystem för informationssäkerhet i enlighet med punkt IS.I.OR.215,

5) definierar och genomför, i enlighet med punkt IS.I.OR.220, de åtgärder som krävs för att upptäcka informationssäkerhetshändelser, identifierar de händelser som anses vara incidenter med en potentiell inverkan på flygsäkerheten med undantag för vad som är tillåtet enligt punkt IS.I.OR.205 e samt hanterar och sköter återställning efter sådana informationssäkerhetsincidenter,

6) genomför de åtgärder som har anmälts av den behöriga myndigheten som en omedelbar reaktion på en informationssäkerhetsincident eller sårbarhet med en inverkan på flygsäkerheten,

7) vidtar lämpliga åtgärder, i enlighet med punkt IS.I.OR.225, för att hantera brister som anmälts av den behöriga myndigheten,

8) genomför ett externt rapporteringssystem i enlighet med punkt IS.I.OR.230 för att den behöriga myndigheten ska kunna vidta lämpliga åtgärder,

9) uppfyller kraven i punkt IS.I.OR.235 när den utkontrakterar någon del av den verksamhet som avses i punkt IS.I.OR.200 till andra organisationer,

10) uppfyller de personalkrav som fastställs i punkt IS.I.OR.240,

11) uppfyller de dokumentationskrav som fastställs i punkt IS.I.OR.245,

12) övervakar att organisationen uppfyller kraven i denna förordning och ger återkoppling om brister till den verksamhetsansvariga chefen för att säkerställa ett effektivt genomförande av korrigerande åtgärder,

13) utan att det påverkar tillämpliga krav på incidentrapportering, skyddar konfidentialiteten för all information som organisationen kan ha mottagit från andra organisationer, i enlighet med informationens känslighetsnivå.

b) För att kontinuerligt uppfylla de krav som avses i artikel 1 ska organisationen genomföra en kontinuerlig förbättringsprocess i enlighet med punkt IS.I.OR.260.

c) Organisationen ska i enlighet med punkt IS.I.OR.250 dokumentera alla centrala processer, förfaranden, roller och ansvarsområden som krävs för att uppfylla kraven i punkt IS.I.OR.200 a samt inrätta en process för att ändra denna dokumentation. Ändringar av dessa processer, förfaranden, roller och ansvarsområden ska hanteras i enlighet med punkt IS.I.OR.255.

d) De processer, förfaranden, roller och ansvarsområden som organisationen inrättat för att uppfylla kraven i punkt IS.I.OR.200 a ska motsvara verksamhetens art och komplexitet, på grundval av en bedömning av de informationssäkerhetsrisker som är förknippade med denna verksamhet, och får integreras i andra befintliga ledningssystem som organisationen redan infört.

e) Utan att det påverkar skyldigheten att uppfylla rapporteringskraven i förordning (EU) nr 376/2014 och kraven i punkt IS.I.OR.200 a.13, får den behöriga myndigheten ge organisationen godkännande att inte genomföra de krav som avses i punkterna a–d och de relaterade kraven i punkterna IS.I.OR.205 till IS.I.OR.260 om organisationen på ett för myndigheten tillfredsställande sätt kan visa att dess verksamhet, anläggningar och resurser, liksom de tjänster som den driver, tillhandahåller, tar emot och upprätthåller, inte utgör några informationssäkerhetsrisker med en potentiell inverkan på flygsäkerheten, vare sig för sig själv eller för andra organisationer. Godkännandet ska baseras på en dokumenterad bedömning av informationssäkerhetsrisker som utförts av organisationen eller en tredje part i enlighet med punkt IS.I.OR.205 och granskats och godkänts av dess behöriga myndighet.

Godkännandets fortsatta giltighet kommer att ses över av den behöriga myndigheten efter den tillämpliga tillsynscykeln och närhelst ändringar genomförs i organisationens arbetsområde.

IS.I.OR.205 Bedömning av informationssäkerhetsrisker

a) Organisationen ska identifiera alla sina delar som skulle kunna utsättas för informationssäkerhetsrisker. Detta ska omfatta

1) organisationens verksamhet, anläggningar och resurser, liksom de tjänster som organisationen driver, tillhandahåller, tar emot eller upprätthåller,

2) den utrustning och information och de system och data som bidrar till att de delar som anges i punkt 1 fungerar.

b) Organisationen ska identifiera de gränssnitt som den har mot andra organisationer och som kan leda till ömsesidig exponering för informationssäkerhetsrisker.

c) När det gäller de delar och gränssnitt som avses i punkterna a och b ska organisationen identifiera de informationssäkerhetsrisker som kan ha en potentiell inverkan på flygsäkerheten. För varje identifierad risk ska organisationen

1) tilldela en risknivå enligt en fördefinierad klassificering som fastställts av organisationen,

2) associera varje risk och dess nivå med motsvarande del eller gränssnitt som identifierats i enlighet med punkterna a och b.

Den fördefinierade klassificering som avses i punkt 1 ska ta hänsyn till risken för att hotscenariot inträffar och hur allvarliga konsekvenser det skulle få för säkerheten. På grundval av denna klassificering, och med beaktande av huruvida organisationen har en strukturerad och repeterbar riskhanteringsprocess för verksamheten, ska organisationen kunna fastställa om risken är acceptabel eller behöver hanteras i enlighet med punkt IS.I.OR.210.

För att underlätta riskbedömningarnas ömsesidiga jämförbarhet ska tilldelningen av risknivå enligt punkt 1 ta hänsyn till relevant information som erhållits i samordning med de organisationer som avses i punkt b.

d) Organisationen ska se över och uppdatera den riskbedömning som utförts i enlighet med punkterna a, b och i tillämpliga fall punkt c eller e, i någon av följande situationer:

1) Det sker en förändring i de delar som omfattas av informationssäkerhetsrisker.

2) Det sker en förändring i gränssnitten mellan organisationen och andra organisationer, eller i de risker som meddelats av de andra organisationerna.

3) Det sker en förändring i den information eller kunskap som används för att identifiera, analysera och klassificera risker.

4) Lärdom dras av analysen av informationssäkerhetsincidenter.

e) Genom undantag från punkt c ska organisationer som är skyldiga att uppfylla kraven i kapitel C i bilaga III (Del-ATM/ANS.OR) till genomförandeförordning (EU) 2017/373 ersätta analysen av inverkan på flygsäkerheten med en analys av inverkan på sina tjänster enligt den stödjande flygsäkerhetsbedömning som krävs enligt punkt ATM/ANS.OR.C.005. Denna stödjande flygsäkerhetsbedömning ska göras tillgänglig för de leverantörer av flygtrafikledningstjänster till vilka de tillhandahåller tjänster, och dessa leverantörer av flygtrafikledningstjänster ska ansvara för utvärderingen av inverkan på flygsäkerheten.

IS.I.OR.210 Hantering av informationssäkerhetsrisker

a) Organisationen ska utarbeta åtgärder för att hantera oacceptabla risker som identifierats i enlighet med punkt IS.I.OR.205, genomföra dem i rätt tid och kontrollera att de fortfarande är effektiva. Dessa åtgärder ska göra det möjligt för organisationen att

1) kontrollera de omständigheter som bidrar till att hotscenariot faktiskt inträffar,

2) minska konsekvenserna för flygsäkerheten i samband med att hotscenariot förverkligas,

3) undvika riskerna.

Dessa åtgärder får inte medföra några nya potentiella oacceptabla risker för flygsäkerheten.

b) Den person som avses i punkt IS.I.OR.240 a och b och annan berörd personal inom organisationen ska informeras om resultatet av den riskbedömning som utförts i enlighet med punkt IS.I.OR.205, motsvarande hotscenarier och de åtgärder som ska vidtas.

Organisationen ska också informera organisationer mot vilka den har ett gränssnitt i enlighet med punkt IS.I.OR.205 b om eventuella risker som är gemensamma för de båda organisationerna.

IS.I.OR.215 Internt rapporteringssystem för informationssäkerhet

a) Organisationen ska inrätta ett internt rapporteringssystem för att möjliggöra insamling och utvärdering av informationssäkerhetshändelser, bland annat de som ska rapporteras enligt punkt IS.I.OR.230.

b) Detta system och den process som avses i punkt IS.I.OR.220 ska göra det möjligt för organisationen att

1) identifiera vilka av de händelser som rapporterats i enlighet med punkt a som anses vara informationssäkerhetsincidenter eller sårbarheter med potentiell inverkan på flygsäkerheten,

2) identifiera orsakerna och bidragande faktorer till de informationssäkerhetsincidenter och sårbarheter som identifierats i enlighet med punkt 1 och ta itu med dem som en del av riskhanteringsprocessen för informationssäkerhet i enlighet med punkterna IS.I.OR.205 och IS.I.OR.220,

3) säkerställa en utvärdering av all känd och relevant information om de informationssäkerhetsincidenter och sårbarheter som identifierats i enlighet med punkt 1,

4) säkerställa genomförandet av en metod för att internt distribuera informationen vid behov.

c) Eventuella underleverantörer som kan utsätta organisationen för informationssäkerhetsrisker med en potentiell inverkan på flygsäkerheten ska vara skyldiga att rapportera informationssäkerhetshändelser till organisationen. Dessa rapporter ska lämnas in enligt de förfaranden som fastställs i de särskilda avtalsarrangemangen och ska utvärderas i enlighet med punkt b.

d) Organisationen ska vid utredningar samarbeta med alla andra organisationer som på ett betydande sätt bidrar till informationssäkerheten för den egna verksamheten.

e) Organisationen får integrera detta rapporteringssystem med andra rapporteringssystem som den redan har infört.

IS.I.OR.220 Informationssäkerhetsincidenter – upptäckt, hantering och återställning

a) På grundval av resultatet av den riskbedömning som utförts i enlighet med punkt IS.I.OR.205 och resultatet av den riskhantering som utförts i enlighet med punkt IS.I.OR.210 ska organisationen vidta åtgärder för att upptäcka incidenter och sårbarheter som visar att oacceptabla risker potentiellt kan förverkligas och som kan ha en potentiell inverkan på flygsäkerheten. Dessa upptäcktsåtgärder ska göra det möjligt för organisationen att

1) identifiera avvikelser från fördefinierade utgångsvärden för funktionsprestanda,

2) utlösa varningar för att aktivera lämpliga reaktionsåtgärder, vid eventuella avvikelser.

b) Organisationen ska vidta åtgärder för att reagera på alla händelseförhållanden som identifierats i enlighet med punkt a och som kan utvecklas eller har utvecklats till en informationssäkerhetsincident. Dessa reaktionsåtgärder ska göra det möjligt för organisationen att

1) inleda reaktionen på de varningar som avses i punkt a.2 genom att aktivera fördefinierade resurser och åtgärder,

2) begränsa spridningen av en attack och undvika att ett hotscenario förverkligas fullt ut,

3) kontrollera felläget för de berörda delar som anges i punkt IS.I.OR.205 a.

c) Organisationen ska vidta åtgärder som syftar till återställning efter informationssäkerhetsincidenter, inbegripet nödåtgärder om så behövs. Dessa återställningsåtgärder ska göra det möjligt för organisationen att

1) eliminera det förhållande som orsakade incidenten eller begränsa det till en acceptabel nivå,

2) uppnå ett säkert tillstånd för de berörda delar som anges i punkt IS.I.OR.205 a inom en återställningstid som tidigare fastställts av organisationen.

IS.I.OR.225 Hantering av brister som anmälts av den behöriga myndigheten

a) Efter att ha mottagit anmälan av brister från den behöriga myndigheten ska organisationen

1) identifiera grundorsaken eller grundorsakerna, samt bidragande faktorer, till den bristande kravuppfyllelsen,

2) utarbeta en plan för korrigerande åtgärder,

3) påvisa att den bristande kravuppfyllelsen har korrigerats på ett för den behöriga myndigheten tillfredsställande sätt.

b) De åtgärder som avses i punkt a ska genomföras inom den tidsfrist som överenskommits med den behöriga myndigheten.

IS.I.OR.230 Externt rapporteringssystem för informationssäkerhet

a) Organisationen ska införa ett rapporteringssystem för informationssäkerhet som uppfyller kraven i förordning (EU) nr 376/2014 och dess delegerade akter och genomförandeakter om den förordningen är tillämplig på organisationen.

b) Utan att det påverkar skyldigheterna enligt förordning (EU) nr 376/2014 ska organisationen säkerställa att alla informationssäkerhetsincidenter eller sårbarheter som kan utgöra en betydande risk för flygsäkerheten rapporteras till dess behöriga myndighet. Dessutom gäller följande:

1) Om en sådan incident eller sårbarhet påverkar ett luftfartyg eller tillhörande system eller komponent ska organisationen också rapportera den till innehavaren av konstruktionsgodkännandet.

2) Om en sådan incident eller sårbarhet påverkar ett system eller en komponent som används av organisationen, ska organisationen rapportera den till den organisation som ansvarar för konstruktionen av systemet eller komponenten.

c) Organisationen ska rapportera de omständigheter som avses i punkt b enligt följande:

1) En anmälan ska lämnas in till den behöriga myndigheten och, i tillämpliga fall, till innehavaren av konstruktionsgodkännandet eller till den organisation som ansvarar för konstruktionen av systemet eller komponenten, så snart som organisationen får kännedom om omständigheterna.

2) En rapport ska lämnas in till den behöriga myndigheten och, i tillämpliga fall, till innehavaren av konstruktionsgodkännandet eller till den organisation som ansvarar för konstruktionen av systemet eller komponenten, så snart som möjligt men senast 72 timmar efter det att organisationen får kännedom om omständigheterna, såvida inte exceptionella omständigheter förhindrar detta.

Rapporten ska göras i den form som fastställs av den behöriga myndigheten och innehålla all relevant information som organisationen känner till om omständigheten.

3) En uppföljningsrapport ska lämnas in till den behöriga myndigheten och, i tillämpliga fall, till innehavaren av konstruktionsgodkännandet eller till den organisation som ansvarar för konstruktionen av systemet eller komponenten, med uppgifter om de åtgärder som organisationen har vidtagit eller avser att vidta för återställning efter incidenten och de åtgärder den avser att vidta för att förhindra liknande informationssäkerhetsincidenter i framtiden.

Uppföljningsrapporten ska lämnas in så snart dessa åtgärder har identifierats och ska utarbetas i den form som fastställs av den behöriga myndigheten.

IS.I.OR.235 Utkontraktering av verksamhet som rör hantering av informationssäkerhet

a) Vid utkontraktering av någon del av den verksamhet som avses i punkt IS.I.OR.200 till andra organisationer ska organisationen säkerställa att den utkontrakterade verksamheten uppfyller kraven i denna förordning och att underleverantören arbetar under dess tillsyn. Organisationen ska säkerställa att de risker som är förenade med den utkontrakterade verksamheten hanteras på lämpligt sätt.

b) Organisationen ska säkerställa att den behöriga myndigheten på begäran kan få tillgång till underleverantören för att fastställa att de tillämpliga kraven i denna förordning fortfarande är uppfyllda.

IS.I.OR.240 Personalkrav

a) Den verksamhetsansvariga chef för organisationen som utsetts i enlighet med förordningarna (EU) nr 1321/2014, (EU) nr 965/2012, (EU) nr 1178/2011, (EU) 2015/340, genomförandeförordning (EU) 2017/373 eller genomförandeförordning (EU) 2021/664, beroende på vad som är tillämpligt enligt artikel 2.1 i den här förordningen, ska ha organisationens bemyndigande att säkerställa att all verksamhet som krävs enligt den här förordningen kan finansieras och genomföras. Denna person ska

1) säkerställa att alla nödvändiga resurser finns tillgängliga för att uppfylla kraven i denna förordning,

2) fastställa och främja den informationssäkerhetspolicy som avses i punkt IS.I.OR.200 a.1,

3) uppvisa en grundläggande förståelse av denna förordning.

b) Den verksamhetsansvariga chefen ska utse en person eller en grupp av personer som ska säkerställa att organisationen uppfyller kraven i denna förordning och ska fastställa omfattningen av deras befogenheter. Denna person eller grupp av personer ska rapportera direkt till den verksamhetsansvariga chefen och ska ha lämplig kunskap, bakgrund och erfarenhet för att kunna fullgöra sitt ansvar. I förfarandena ska det fastställas vem som vikarierar för en viss person om den personen är frånvarande under längre tid.

c) Den verksamhetsansvariga chefen ska utse en person eller en grupp av personer som har ansvaret för att hantera den funktion för övervakning av kravuppfyllelse som avses i punkt IS.I.OR.200 a.12.

d) Om organisationen delar organisatoriska strukturer, policyer, processer och förfaranden för informationssäkerhet med andra organisationer eller med delar av den egna organisationen som inte omfattas av godkännandet eller försäkran, får den verksamhetsansvariga chefen delegera verksamheten till en gemensam ansvarig person.

I sådana fall ska samordningsåtgärder fastställas mellan organisationens verksamhetsansvariga chef och den gemensamma ansvariga personen för att säkerställa att hanteringen av informationssäkerhet integreras på lämpligt sätt inom organisationen.

e) Den verksamhetsansvariga chefen eller den gemensamma ansvariga person som avses i punkt d ska ha organisationens bemyndigande att upprätta och upprätthålla de organisatoriska strukturer, policyer, processer och förfaranden som krävs för att genomföra punkt IS.I.OR.200.

f) Organisationen ska ha en process för att säkerställa att den har tillräckligt med personal i tjänst för att kunna utföra den verksamhet som omfattas av denna bilaga.

g) Organisationen ska ha en process för att säkerställa att den personal som avses i punkt f har den kompetens som krävs för att utföra uppgifterna.

h) Organisationen ska ha en process för att säkerställa att personalen är medveten om det ansvar som är förenat med de tilldelade rollerna och uppgifterna.

i) Organisationen ska säkerställa att identiteten på och tillförlitligheten hos den personal som har åtkomst till informationssystem och data som omfattas av kraven i denna förordning fastställs på lämpligt sätt.

IS.I.OR.245 Dokumentation

a) *Organisationen ska dokumentera sin verksamhet för hantering av informationssäkerhet.*

1) Organisationen ska säkerställa att följande dokumentation arkiveras och kan spåras:

i) Alla godkännanden som mottagits och eventuella tillhörande bedömningar av informationssäkerhetsrisker i enlighet med punkt IS.I.OR.200 e.

ii) Kontrakt för verksamhet som avses i punkt IS.I.OR.200 a.9.

iii) Dokumentation av de centrala processer som avses i punkt IS.I.OR.200 d.

iv) Dokumentation av de risker som identifierats i den riskbedömning som avses i punkt IS.I.OR.205 tillsammans med de tillhörande riskhanteringsåtgärder som avses i punkt IS.I.OR.210.

v) Dokumentation av informationssäkerhetsincidenter och sårbarheter som rapporterats i enlighet med de rapporteringssystem som avses i punkterna IS.I.OR.215 och IS.I.OR.230.

vi) Dokumentation av de informationssäkerhetshändelser som kan behöva omprövas för att avslöja oupptäckta informationssäkerhetsincidenter eller sårbarheter.

2) Den dokumentation som avses i punkt 1 i ska bevaras i minst fem år efter det att godkännandet inte längre än giltigt.

3) Den dokumentation som avses i punkt 1 ii ska bevaras i minst fem år efter det att kontraktet har ändrats eller sagts upp.

4) Den dokumentation som avses i punkt 1 iii, iv och v ska bevaras i minst fem år.

5) Den dokumentation som avses i punkt 1 vi ska bevaras till dess att dessa informationssäkerhetshändelser har omprövats i enlighet med en periodicitet som anges i ett förfarande som fastställts av organisationen.

b) *Organisationen ska ha dokumentation över kvalifikationer och erfarenhet när det gäller den egna personalen som arbetar med hantering av informationssäkerhet*.

1) Dokumentationen av personalens kvalifikationer och erfarenhet ska bevaras så länge personen arbetar för organisationen och i minst tre år efter det att personen har lämnat organisationen.

2) Anställda ska på egen begäran få tillgång till den dokumentation som gäller dem. På deras begäran ska organisationen också ge dem en kopia av den dokumentation som gäller dem när de lämnar organisationen.

c) Formatet för dokumentationen ska anges i organisationens förfaranden.

d) Dokumentationen ska lagras på ett sätt som säkerställer skydd från skada, ändring och stöld, vid behov med uppgift om informationens säkerhetsskyddsklassificeringsnivå. Organisationen ska säkerställa att dokumentationen lagras på ett sätt som säkerställer integritet, autenticitet och behörig åtkomst.

IS.I.OR.250 Handbok för hantering av informationssäkerhet (ISMM)

a) Organisationen ska förse den behöriga myndigheten med en handbok för hantering av informationssäkerhet (ISMM) och, i tillämpliga fall, eventuella tillhörande manualer och förfaranden, med följande uppgifter:

1) En försäkran undertecknad av den verksamhetsansvariga chefen som bekräftar att organisationen alltid kommer att utföra sin verksamhet i enlighet med denna bilaga och ISMM. Om den verksamhetsansvariga chefen inte är organisationens verkställande direktör ska den verkställande direktören kontrasignera försäkran.

2) Titlar, namn, arbetsuppgifter, skyldigheter, ansvar och befogenheter för den eller de personer som avses i punkt IS.I.OR.240 b och c.

3) Titlar, namn, arbetsuppgifter, skyldigheter, ansvar och befogenheter för den gemensamma ansvariga person som avses i punkt IS.I.OR.240 d, i tillämpliga fall.

4) Organisationens informationssäkerhetspolicy som avses i punkt IS.I.OR.200 a.1.

5) En allmän beskrivning av antalet anställda och personalkategorierna samt det system som finns för att planera personalens tillgänglighet i enlighet med punkt IS.I.OR.240.

6) Titlar, namn, arbetsuppgifter, skyldigheter, ansvar och befogenheter för de centrala personer som ansvarar för genomförandet av punkt IS.I.OR.200, inbegripet den eller de personer som ansvarar för övervakning av kravuppfyllelse enligt punkt IS.I.OR.200 a.12.

7) Ett organisationsschema som visar tillhörande kedjor av ansvarsskyldighet och ansvar för de personer som avses i punkterna 2 och 6.

8) Beskrivningen av det interna rapporteringssystem som avses i punkt IS.I.OR.215.

9) De förfaranden som specificerar hur organisationen säkerställer efterlevnad av denna del, särskilt

i) den dokumentation som avses i punkt IS.I.OR.200 c,

ii) de förfaranden som definierar hur organisationen kontrollerar eventuell utkontrakterad verksamhet enligt vad som avses i punkt IS.I.OR.200 a.9,

iii) det förfarande för ISMM-ändring som avses i punkt c.

10) Uppgifter om de för närvarande godkända alternativa sätten att uppfylla kraven.

b) Det första utfärdandet av ISMM ska godkännas och en kopia ska behållas av den behöriga myndigheten. ISMM ska vid behov ändras så att den förblir en aktuell beskrivning av organisationens ISMS. En kopia av eventuella ändringar av ISMM ska lämnas till den behöriga myndigheten.

c) Ändringar av ISMM ska hanteras enligt ett förfarande som fastställs av organisationen. Ändringar som inte omfattas av detta förfarande och eventuella ändringar som rör de ändringar som avses i punkt IS.I.OR.255 b ska godkännas av den behöriga myndigheten.

d) Organisationen får integrera ISMM med sina andra ledningshandböcker eller handledningar, förutsatt att det finns en tydlig korshänvisning som anger vilka delar av ledningshandboken eller handledningen som motsvarar de olika kraven i denna bilaga.

IS.I.OR.255 Ändringar av systemet för hantering av informationssäkerhet

a) Ändringar av ISMS får hanteras och anmälas till den behöriga myndigheten genom ett förfarande som utarbetats av organisationen. Detta förfarande ska godkännas av den behöriga myndigheten.

b) När det gäller ändringar av ISMS som inte omfattas av det förfarande som avses i punkt a ska organisationen ansöka om och erhålla ett godkännande från den behöriga myndigheten.

För dessa ändringar gäller följande:

1) Ansökan ska lämnas in innan någon ändring äger rum för att den behöriga myndigheten ska kunna fastställa fortsatt efterlevnad av denna förordning samt vid behov ändra organisationens certifikat och de villkor för godkännande som bifogas certifikatet.

2) Organisationen ska ge den behöriga myndigheten tillgång till all information den begär för att kunna utvärdera ändringen.

3) Ändringen ska genomföras först efter att ett formellt godkännande har mottagits från den behöriga myndigheten.

4) Vid genomförandet av sådana ändringar ska organisationen agera enligt de villkor som föreskrivs av den behöriga myndigheten.

IS.I.OR.260 Löpande förbättring

a) Organisationen ska med hjälp av lämpliga resultatindikatorer bedöma ISMS effektivitet och mognadsgrad. Bedömningen ska utföras enligt en tidsplan som fastställts på förhand av organisationen eller till följd av en informationssäkerhetsincident.

b) Om brister upptäcks till följd av den bedömning som utförts i enlighet med punkt a ska organisationen vidta nödvändiga förbättringsåtgärder för att säkerställa att ISMS fortsätter att uppfylla de tillämpliga kraven och upprätthåller en acceptabel nivå för informationssäkerhetsriskerna. Dessutom ska organisationen göra en ny bedömning av de delar av ISMS som påverkas av de antagna åtgärderna.

BILAGA III

Bilagorna VI (Del-ARA) och VII (Del-ORA) till förordning (EU) nr 1178/2011 ska ändras på följande sätt:

(1) Bilaga VI (Del ARA) ska ändras på följande sätt:

(a) I punkt ARA.GEN.125 ska följande punkt läggas till som punkt c:

"c) Medlemsstatens behöriga myndighet ska så snart som möjligt förse byrån med information av betydelse för säkerheten som härrör från de informationssäkerhetsrapporter som den har mottagit enligt punkt IS.I.OR.230 i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203."

(b) Efter punkt ARA.GEN.135 ska följande punkt införas som punkt ARA.GEN.135A:

"**ARA.GEN.135A Omedelbar reaktion på en informationssäkerhetsincident eller sårbarhet med en inverkan på flygsäkerheten**

a) Den behöriga myndigheten ska införa ett system för att på lämpligt sätt samla in, analysera och sprida information om informationssäkerhetsincidenter och sårbarheter med en potentiell inverkan på flygsäkerheten som rapporteras av organisationer. Detta ska göras i samordning med andra relevanta myndigheter som ansvarar för informationssäkerhet eller cybersäkerhet i medlemsstaten för att öka samordningen av och förenligheten hos rapporteringssystemen.

b) Byrån ska införa ett system för att på lämpligt sätt analysera all relevant information av betydelse för säkerheten som mottagits i enlighet med punkt ARA.GEN.125 c och utan onödigt dröjsmål förse medlemsstaterna och kommissionen med all information, inklusive rekommendationer eller korrigerande åtgärder som ska vidtas, som krävs för att de i god tid ska kunna reagera på en informationssäkerhetsincident eller sårbarhet med en potentiell inverkan på flygsäkerheten som inbegriper produkter, delar, utrustning som inte är fast installerad, personer eller organisationer som omfattas av förordning (EU) 2018/1139 och dess delegerade akter och genomförandeakter.

c) När den behöriga myndigheten har mottagit den information som avses i punkterna a och b ska den vidta lämpliga åtgärder för att ta itu med den potentiella inverkan av informationssäkerhetsincidenten eller sårbarheten på flygsäkerheten.

d) Åtgärder som vidtas i enlighet med punkt c ska omgående meddelas alla personer eller organisationer som ska följa dem enligt förordning (EU) 2018/1139 och dess delegerade akter och genomförandeakter. Medlemsstatens behöriga myndighet ska också informera byrån och, om kombinerade åtgärder krävs, de behöriga myndigheterna i övriga berörda medlemsstater, om dessa åtgärder."

(c) I punkt ARA.GEN.200 ska följande punkt läggas till som punkt e:

"e) Utöver kraven i punkt a ska det ledningssystem som inrättats och upprätthålls av den behöriga myndigheten uppfylla kraven i bilaga I (Del-IS.AR) till genomförandeförordning (EU) 2023/203 för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten."

(d) Punkt ARA.GEN.205 ska ändras på följande sätt:

i) Rubriken ska ersättas med följande:

"**ARA.GEN.205 Tilldelning av uppgifter**".

ii) Följande punkt ska läggas till som punkt c:

"c) När det gäller certifiering och tillsyn av organisationens efterlevnad av punkt ORA.GEN.200A får den behöriga myndigheten tilldela uppgifter till behöriga organ i enlighet med punkt a eller till en relevant myndighet som ansvarar för informationssäkerhet eller cybersäkerhet i medlemsstaten. När den behöriga myndigheten tilldelar uppgifter ska den säkerställa att

1) alla aspekter som rör flygsäkerheten samordnas och beaktas av det behöriga organet eller den relevanta myndigheten,

2) resultaten av den certifiering och tillsyn som utförs av det behöriga organet eller den relevanta myndigheten integreras i den övergripande certifierings- och tillsynsdokumentationen för organisationen,

3) det egna systemet för hantering av informationssäkerhet, som inrättats i enlighet med punkt ARA.GEN.200 e, omfattar alla arbetsuppgifter i samband med certifiering och fortlöpande tillsyn som utförs för dess räkning."

(e) I punkt ARA.GEN.300 ska följande punkt läggas till som punkt g:

"g) När det gäller certifiering och tillsyn av organisationens efterlevnad av punkt ORA.GEN.200A ska den behöriga myndigheten, utöver att uppfylla kraven i punkterna a–f, se över alla godkännanden som beviljats enligt punkt IS.I.OR.200 e i denna förordning eller punkt IS.D.OR.200 e i delegerad förordning (EU) 2022/1645 efter den tillämpliga tillsynscykeln och närhelst ändringar genomförs i organisationens arbetsområde."

(f) Efter punkt ARA.GEN.330 ska följande punkt införas som punkt ARA.GEN.330A:

"**ARA.GEN.330A Ändringar av systemet för hantering av informationssäkerhet**

a) För ändringar som hanteras och anmäls till den behöriga myndigheten i enlighet med förfarandet i punkt IS.I.OR.255 a i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203 ska den behöriga myndigheten inkludera en översyn av sådana ändringar i sin fortlöpande tillsyn i enlighet med principerna i punkt ARA.GEN.300. Om bristande efterlevnad konstateras ska den behöriga myndigheten underrätta organisationen om detta, begära ytterligare ändringar och agera i enlighet med punkt ARA.GEN.350.

b) För andra ändringar som kräver en ansökan om godkännande i enlighet med punkt IS.I.OR.255 b i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203 gäller följande:

1) När den behöriga myndigheten har mottagit ansökan om ändring ska den, innan den utfärdar ett godkännande, kontrollera att organisationen uppfyller de tillämpliga kraven.

2) Den behöriga myndigheten ska fastställa de villkor enligt vilka organisationen får verka under genomförandet av ändringen.

3) Efter att ha försäkrat sig om att organisationen uppfyller de tillämpliga kraven ska den behöriga myndigheten godkänna ändringen."

(2) Bilaga VII (Del-ORA) ska ändras på följande sätt:

Efter punkt ORA.GEN.200 ska följande punkt införas som punkt ORA.GEN.200A:

"**ORA.GEN.200A System för hantering av informationssäkerhet**

Utöver det ledningssystem som avses i punkt ORA.GEN.200 ska organisationen inrätta, genomföra och upprätthålla ett system för hantering av informationssäkerhet i enlighet med genomförandeförordning (EU) 2023/203 för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten."

BILAGA IV

Bilaga I (Del 21) till förordning (EU) nr 748/2012 ska ändras på följande sätt:

(1) Innehållsförteckningen ska ändras på följande sätt:

(a) Följande rubrik ska införas efter rubrik 21.B.20:

”21.B.20A Omedelbar reaktion på en informationssäkerhetsincident eller sårbarhet med en inverkan på flygsäkerheten”.

(b) Rubriken till punkt 21.B.30 ska ersättas med följande:

”21.B.30 Tilldelning av uppgifter”.

(c) Följande rubrik ska införas efter rubrik 21.B.240:

”21.B.240A Ändringar av systemet för hantering av informationssäkerhet”.

(d) Följande rubrik ska införas efter rubrik 21.B.435:

”21.B.435A Ändringar av systemet för hantering av informationssäkerhet”.

(2) I punkt 21.B.15 ska följande punkt läggas till som punkt c:

”c) Medlemsstatens behöriga myndighet ska så snart som möjligt förse byrån med information av betydelse för säkerheten som härrör från de informationssäkerhetsrapporter som den har mottagit enligt punkt IS.D.OR.230 i bilagan (Del-IS.D.OR) till delegerad förordning (EU) 2022/1645.”

(3) Efter punkt 21.B.20 ska följande punkt införas som punkt 21.B.20A:

”21.B.20A Omedelbar reaktion på en informationssäkerhetsincident eller sårbarhet med en inverkan på flygsäkerheten

a) Den behöriga myndigheten ska införa ett system för att på lämpligt sätt samla in, analysera och sprida information om informationssäkerhetsincidenter och sårbarheter med en potentiell inverkan på flygsäkerheten som rapporteras av organisationer. Detta ska göras i samordning med andra relevanta myndigheter som ansvarar för informationssäkerhet eller cybersäkerhet i medlemsstaten för att öka samordningen av och förenligheten hos rapporteringssystemen.

b) Byrån ska införa ett system för att på lämpligt sätt analysera all relevant information av betydelse för säkerheten som mottagits i enlighet med punkt 21.B.15 c och utan onödigt dröjsmål förse medlemsstaterna och kommissionen med all information, inklusive rekommendationer eller korrigerande åtgärder som ska vidtas, som krävs för att de i god tid ska kunna reagera på en informationssäkerhetsincident eller sårbarhet med en potentiell inverkan på flygsäkerheten som inbegriper produkter, delar, utrustning som inte är fast installerad, personer eller organisationer som omfattas av förordning (EU) 2018/1139 och dess delegerade akter och genomförandeakter.

c) När den behöriga myndigheten har mottagit den information som avses i punkterna a och b ska den vidta lämpliga åtgärder för att ta itu med den potentiella inverkan av informationssäkerhetsincidenten eller sårbarheten på flygsäkerheten.

d) Åtgärder som vidtas i enlighet med punkt c ska omgående meddelas alla personer eller organisationer som ska följa dem enligt förordning (EU) 2018/1139 och dess delegerade akter och genomförandeakter. Medlemsstatens behöriga myndighet ska också informera byrån och, om kombinerade åtgärder krävs, de behöriga myndigheterna i övriga berörda medlemsstater, om dessa åtgärder.”

(4) I punkt 21.B.25 ska följande punkt läggas till som punkt e:

”e) Utöver kraven i punkt a ska det ledningssystem som inrättats och upprätthålls av den behöriga myndigheten uppfylla kraven i bilaga I (Del-IS.AR) till genomförandeförordning (EU) 2023/203 för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten.”

(5) Punkt 21.B.30 ska ändras på följande sätt:

(a) Rubriken ska ersättas med följande:

”21.B.30 Tilldelning av uppgifter”.

(b) Följande punkt ska läggas till som punkt c:

”c) När det gäller certifiering och tillsyn av organisationens efterlevnad av punkterna 21.A.139A och 21.A.239A får den behöriga myndigheten tilldela uppgifter till behöriga organ i enlighet med punkt a eller till en relevant myndighet som ansvarar för informationssäkerhet eller cybersäkerhet i medlemsstaten. När den behöriga myndigheten tilldelar uppgifter ska den säkerställa att

1) alla aspekter som rör flygsäkerheten samordnas och beaktas av det behöriga organet eller den relevanta myndigheten,

2) resultaten av den certifiering och tillsyn som utförs av det behöriga organet eller den relevanta myndigheten integreras i den övergripande certifierings- och tillsynsdokumentationen för organisationen,

3) det egna systemet för hantering av informationssäkerhet, som inrättats i enlighet med punkt 21.B.25 e, omfattar alla arbetsuppgifter i samband med certifiering och fortlöpande tillsyn som utförs för dess räkning.”

(6) I punkt 21.B.221 ska följande punkt läggas till som punkt g:

”g) När det gäller certifiering och tillsyn av organisationens efterlevnad av punkt 21.A.139A ska den behöriga myndigheten, utöver att uppfylla kraven i punkterna a–f, se över alla godkännanden som beviljats enligt punkt IS.I.OR.200 e i denna förordning eller punkt IS.D.OR.200 e i delegerad förordning (EU) 2022/1645 efter den tillämpliga tillsynscykeln och närhelst ändringar genomförs i organisationens arbetsområde.”

(7) Efter punkt 21.B.240 ska följande punkt införas som punkt 21.B.240A:

”**21.B.240A Ändringar av systemet för hantering av informationssäkerhet**

a) För ändringar som hanteras och anmäls till den behöriga myndigheten i enlighet med förfarandet i punkt IS.D.OR.255 a i bilagan (Del-IS.D.OR) till delegerad förordning (EU) 2022/1645 ska den behöriga myndigheten inkludera en översyn av sådana ändringar i sin fortlöpande tillsyn i enlighet med principerna i punkt 21.B.221. Om bristande efterlevnad konstateras ska den behöriga myndigheten underrätta organisationen om detta, begära ytterligare ändringar och agera i enlighet med punkt 21.B.225.

b) För andra ändringar som kräver en ansökan om godkännande i enlighet med punkt IS.D.OR.255 b i bilagan (Del-IS.D.OR) till delegerad förordning (EU) 2022/1645 gäller följande:

1) När den behöriga myndigheten har mottagit ansökan om ändring ska den, innan den utfärdar ett godkännande, kontrollera att organisationen uppfyller de tillämpliga kraven.

2) Den behöriga myndigheten ska fastställa de villkor enligt vilka organisationen får verka under genomförandet av ändringen.

3) Efter att ha försäkrat sig om att organisationen uppfyller de tillämpliga kraven ska den behöriga myndigheten godkänna ändringen.”

(8) I punkt 21.B.431 ska följande punkt läggas till som punkt d:

”d) När det gäller certifiering och tillsyn av organisationens efterlevnad av punkt 21.A.239A ska den behöriga myndigheten, utöver att uppfylla kraven i punkterna a–c, iaktta följande principer:

1) Den behöriga myndigheten ska se över de gränssnitt och tillhörande risker som identifierats i enlighet med punkt IS.D.OR.205 b i bilagan (Del-IS.D.OR) till delegerad förordning (EU) 2022/1645 av varje organisation som står under dess tillsyn.

2) Om avvikelser konstateras i de gemensamma gränssnitt och tillhörande risker som identifierats av olika organisationer ska den behöriga myndigheten se över dem med de berörda organisationerna och vid behov ta upp lämpliga iakttagelser för att säkerställa genomförandet av korrigerande åtgärder.

3) Om det av den dokumentation som setts över i enlighet med punkt 2 framgår att det föreligger betydande risker kopplade till gränssnitt mot organisationer som står under tillsyn av en annan behörig myndighet i samma medlemsstat, ska denna information meddelas motsvarande behöriga myndighet."

(9) Efter punkt 21.B.435 ska följande punkt införas som punkt 21.B.435A:

"**21.B.435A Ändringar av systemet för hantering av informationssäkerhet**

a) För ändringar som hanteras och anmäls till den behöriga myndigheten i enlighet med förfarandet i punkt IS.D.OR.255 a i bilagan (Del-IS.D.OR) till delegerad förordning (EU) 2022/1645 ska den behöriga myndigheten inkludera en översyn av sådana ändringar i sin fortlöpande tillsyn i enlighet med principerna i punkt 21.B.431. Om bristande efterlevnad konstateras ska den behöriga myndigheten underrätta organisationen om detta, begära ytterligare ändringar och agera i enlighet med punkt 21.B.433.

b) För andra ändringar som kräver en ansökan om godkännande i enlighet med punkt IS.D.OR.255 b i bilagan (Del-IS.D.OR) till delegerad förordning (EU) 2022/1645 gäller följande:

1) När den behöriga myndigheten har mottagit ansökan om ändring ska den, innan den utfärdar ett godkännande, kontrollera att organisationen uppfyller de tillämpliga kraven.

2) Den behöriga myndigheten ska fastställa de villkor enligt vilka organisationen får verka under genomförandet av ändringen.

3) Efter att ha försäkrat sig om att organisationen uppfyller de tillämpliga kraven ska den behöriga myndigheten godkänna ändringen."

BILAGA V

Bilagorna II (Del-ARO) och III (Del-ORO) till förordning (EU) nr 965/2012 ska ändras på följande sätt:

(1) Bilaga II (Del-ARO) ska ändras på följande sätt:

(a) I punkt ARO.GEN.125 ska följande punkt läggas till som punkt c:

”c) Medlemsstatens behöriga myndighet ska så snart som möjligt förse byrån med information av betydelse för säkerheten som härrör från de informationssäkerhetsrapporter som den har mottagit enligt punkt IS.I.OR.230 i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203.”

(b) Efter punkt ARO.GEN.135 ska följande punkt införas som punkt ARO.GEN.135A:

”**ARO.GEN.135A Omedelbar reaktion på en informationssäkerhetsincident eller sårbarhet med en inverkan på flygsäkerheten**

a) Den behöriga myndigheten ska införa ett system för att på lämpligt sätt samla in, analysera och sprida information om informationssäkerhetsincidenter och sårbarheter med en potentiell inverkan på flygsäkerheten som rapporteras av organisationer. Detta ska göras i samordning med andra relevanta myndigheter som ansvarar för informationssäkerhet eller cybersäkerhet i medlemsstaten för att öka samordningen av och förenligheten hos rapporteringssystemen.

b) Byrån ska införa ett system för att på lämpligt sätt analysera all relevant information av betydelse för säkerheten som mottagits i enlighet med punkt ARO.GEN.125 c och utan onödigt dröjsmål förse medlemsstaterna och kommissionen med all information, inklusive rekommendationer eller korrigerande åtgärder som ska vidtas, som krävs för att de i god tid ska kunna reagera på en informationssäkerhetsincident eller sårbarhet med en potentiell inverkan på flygsäkerheten som inbegriper produkter, delar, utrustning som inte är fast installerad, personer eller organisationer som omfattas av förordning (EU) 2018/1139 och dess delegerade akter och genomförandeakter.

c) När den behöriga myndigheten har mottagit den information som avses i punkterna a och b ska den vidta lämpliga åtgärder för att ta itu med den potentiella inverkan av informationssäkerhetsincidenten eller sårbarheten på flygsäkerheten.

d) Åtgärder som vidtas i enlighet med punkt c ska omgående meddelas alla personer eller organisationer som ska följa dem enligt förordning (EU) 2018/1139 och dess delegerade akter och genomförandeakter. Medlemsstatens behöriga myndighet ska också informera byrån och, om kombinerade åtgärder krävs, de behöriga myndigheterna i övriga berörda medlemsstater, om dessa åtgärder.”

(c) I punkt ARO.GEN.200 ska följande punkt läggas till som punkt e:

”e) Utöver kraven i punkt a ska det ledningssystem som inrättats och upprätthålls av den behöriga myndigheten uppfylla kraven i bilaga I (Del-IS.AR) till genomförandeförordning (EU) 2023/203 för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten.”

(d) Punkt ARO.GEN.205 ska ändras på följande sätt:

(i) Rubriken ska ersättas med följande:

”**ARO.GEN.205 Tilldelning av uppgifter**”.

(ii) Följande punkt ska läggas till som punkt c:

"c) När det gäller certifiering och tillsyn av organisationens efterlevnad av punkt ORO.GEN.200A får den behöriga myndigheten tilldela uppgifter till behöriga organ i enlighet med punkt a eller till en relevant myndighet som ansvarar för informationssäkerhet eller cybersäkerhet i medlemsstaten. När den behöriga myndigheten tilldelar uppgifter ska den säkerställa att

1) alla aspekter som rör flygsäkerheten samordnas och beaktas av det behöriga organet eller den relevanta myndigheten,

2) resultaten av den certifiering och tillsyn som utförs av det behöriga organet eller den relevanta myndigheten integreras i den övergripande certifierings- och tillsynsdokumentationen för organisationen,

3) det egna systemet för hantering av informationssäkerhet, som inrättats i enlighet med punkt ARO.GEN.200 e, omfattar alla arbetsuppgifter i samband med certifiering och fortlöpande tillsyn som utförs för dess räkning."

(e) I punkt ARO.GEN.300 ska följande punkt läggas till som punkt g:

"g) När det gäller certifiering och tillsyn av organisationens efterlevnad av punkt ORO.GEN.200A ska den behöriga myndigheten, utöver att uppfylla kraven i punkterna a–f, se över alla godkännanden som beviljats enligt punkt IS.I.OR.200 e i denna förordning eller punkt IS.D.OR.200 e i delegerad förordning (EU) 2022/1645 efter den tillämpliga tillsynscykeln och närhelst ändringar genomförs i organisationens arbetsområde."

(f) Efter punkt ARO.GEN.330 ska följande punkt införas som punkt ARO.GEN.330A:

"**ARO.GEN.330A Ändringar av systemet för hantering av informationssäkerhet**

a) För ändringar som hanteras och anmäls till den behöriga myndigheten i enlighet med förfarandet i punkt IS.I.OR.255 a i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203 ska den behöriga myndigheten inkludera en översyn av sådana ändringar i sin fortlöpande tillsyn i enlighet med principerna i punkt ARO.GEN.300. Om bristande efterlevnad konstateras ska den behöriga myndigheten underrätta organisationen om detta, begära ytterligare ändringar och agera i enlighet med punkt ARO.GEN.350.

b) För andra ändringar som kräver en ansökan om godkännande i enlighet med punkt IS.I.OR.255 b i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203 gäller följande:

1) När den behöriga myndigheten har mottagit ansökan om ändring ska den, innan den utfärdar ett godkännande, kontrollera att organisationen uppfyller de tillämpliga kraven.

2) Den behöriga myndigheten ska fastställa de villkor enligt vilka organisationen får verka under genomförandet av ändringen.

3) Efter att ha försäkrat sig om att organisationen uppfyller de tillämpliga kraven ska den behöriga myndigheten godkänna ändringen."

(2) Bilaga III (Del-ORO) ska ändras på följande sätt:

Efter punkt ORO.GEN.200 ska följande punkt införas som punkt ORO.GEN.200A:

"**ORO.GEN.200A System för hantering av informationssäkerhet**

Utöver det ledningssystem som avses i punkt ORO.GEN.200 ska operatören inrätta, genomföra och upprätthålla ett system för hantering av informationssäkerhet i enlighet med genomförandeförordning (EU) 2023/203 för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten."

BILAGA VI

Bilaga II (Del-ADR.AR) till förordning (EU) nr 139/2014 ska ändras på följande sätt:

(1) I punkt ADR.AR.A.025 ska följande punkt läggas till som punkt c:

”c) Medlemsstatens behöriga myndighet ska så snart som möjligt förse byrån med information av betydelse för säkerheten som härrör från de informationssäkerhetsrapporter som den har mottagit enligt punkt IS.D.OR.230 i bilagan (Del-IS.D.OR) till delegerad förordning (EU) 2022/1645.”

(2) Efter punkt ADR.AR.A.030 ska följande punkt införas som punkt ADR.AR.A.030A:

”**ADR.AR.A.030A Omedelbar reaktion på en informationssäkerhetsincident eller sårbarhet med en inverkan på flygsäkerheten**

a) Den behöriga myndigheten ska införa ett system för att på lämpligt sätt samla in, analysera och sprida information om informationssäkerhetsincidenter och sårbarheter med en potentiell inverkan på flygsäkerheten som rapporteras av organisationer. Detta ska göras i samordning med andra relevanta myndigheter som ansvarar för informationssäkerhet eller cybersäkerhet i medlemsstaten för att öka samordningen av och förenligheten hos rapporteringssystemen.

b) Byrån ska införa ett system för att på lämpligt sätt analysera all relevant information av betydelse för säkerheten som mottagits i enlighet med punkt ADR.AR.A.025 c och utan onödigt dröjsmål förse medlemsstaterna och kommissionen med all information, inklusive rekommendationer eller korrigerande åtgärder som ska vidtas, som krävs för att de i god tid ska kunna reagera på en informationssäkerhetsincident eller sårbarhet med en potentiell inverkan på flygsäkerheten som inbegriper produkter, delar, utrustning som inte är fast installerad, personer eller organisationer som omfattas av förordning (EU) 2018/1139 och dess delegerade akter och genomförandeakter.

c) När den behöriga myndigheten har mottagit den information som avses i punkterna a och b ska den vidta lämpliga åtgärder för att ta itu med den potentiella inverkan av informationssäkerhetsincidenten eller sårbarheten på flygsäkerheten.

d) Åtgärder som vidtas i enlighet med punkt c ska omgående meddelas alla personer eller organisationer som ska följa dem enligt förordning (EU) 2018/1139 och dess delegerade akter och genomförandeakter. Medlemsstatens behöriga myndighet ska också informera byrån och, om kombinerade åtgärder krävs, de behöriga myndigheterna i övriga berörda medlemsstater, om dessa åtgärder.”

(3) I punkt ADR.AR.B.005 ska följande punkt läggas till som punkt d:

”d) Utöver kraven i punkt a ska det ledningssystem som inrättats och upprätthålls av den behöriga myndigheten uppfylla kraven i bilaga I (Del-IS.AR) till genomförandeförordning (EU) 2023/203 för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten.”

(4) Punkt ADR.AR.B.010 ska ändras på följande sätt:

(i) Rubriken ska ersättas med följande:

”**ADR.AR.B.010 Tilldelning av uppgifter**”.

(ii) Följande punkt ska läggas till som punkt c:

”c) När det gäller certifiering och tillsyn av organisationens efterlevnad av punkt ADR.OR.D.005A får den behöriga myndigheten tilldela uppgifter till behöriga organ i enlighet med punkt a eller till en relevant myndighet som ansvarar för informationssäkerhet eller cybersäkerhet i medlemsstaten. När den behöriga myndigheten tilldelar uppgifter ska den säkerställa att

1) alla aspekter som rör flygsäkerheten samordnas och beaktas av det behöriga organet eller den relevanta myndigheten,

2) resultaten av den certifiering och tillsyn som utförs av det behöriga organet eller den relevanta myndigheten integreras i den övergripande certifierings- och tillsynsdokumentationen för organisationen,

3) det egna systemet för hantering av informationssäkerhet, som inrättats i enlighet med punkt ADR.AR.B.005 e, omfattar alla arbetsuppgifter i samband med certifiering och fortlöpande tillsyn som utförs för dess räkning."

(5) I punkt ADR.AR.C.005 ska följande punkt läggas till som punkt f:

"f) När det gäller certifiering och tillsyn av organisationens efterlevnad av punkt ADR.OR.D.005A ska den behöriga myndigheten, utöver att uppfylla kraven i punkterna a–e, se över alla godkännanden som beviljats enligt punkt IS.I.OR.200 e i denna förordning eller punkt IS.D.OR.200 e i delegerad förordning (EU) 2022/1645 efter den tillämpliga tillsynscykeln och närhelst ändringar genomförs i organisationens arbetsområde."

(6) Efter punkt ADR.AR.C.040 ska följande punkt införas som punkt ADR.AR.C.040A:

"**ADR.AR.C.040A Ändringar av systemet för hantering av informationssäkerhet**

a) När det gäller ändringar som hanteras och anmäls till den behöriga myndigheten i enlighet med förfarandet i punkt IS.D.OR.255 a i bilagan (Del-IS.D.OR) till delegerad förordning (EU) 2022/1645 ska den behöriga myndigheten inkludera en översyn av sådana ändringar i sin fortlöpande tillsyn i enlighet med principerna i punkt ADR.AR.C.005. Om bristande efterlevnad konstateras ska den behöriga myndigheten underrätta organisationen om detta, begära ytterligare ändringar och agera i enlighet med punkt ADR.AR.C.055.

b) När det gäller andra ändringar som kräver en ansökan om godkännande i enlighet med punkt IS.D.OR.255 b i bilagan (Del-IS.D.OR) till delegerad förordning (EU) 2022/1645 gäller följande:

1) När den behöriga myndigheten har mottagit ansökan om ändring ska den, innan den utfärdar ett godkännande, kontrollera att organisationen uppfyller de tillämpliga kraven.

2) Den behöriga myndigheten ska fastställa de villkor enligt vilka organisationen får verka under genomförandet av ändringen.

3) Efter att ha försäkrat sig om att organisationen uppfyller de tillämpliga kraven ska den behöriga myndigheten godkänna ändringen."

BILAGA VII

Bilagorna II (Del-145), III (Del-66) och Vc (Del-CAMO) till förordning (EU) nr 1321/2014 ska ändras på följande sätt:

(1) Bilaga II (Del-145) ska ändras på följande sätt:

(a) Innehållsförteckningen ska ändras på följande sätt:

(i) Följande rubrik ska införas efter rubrik 145.A.200:

”145.A.200A System för hantering av informationssäkerhet”.

(ii) Följande rubrik ska införas efter rubrik 145.B.135:

”145.B.135A Omedelbar reaktion på en informationssäkerhetsincident eller sårbarhet med en inverkan på flygsäkerheten”.

(iii) Rubriken till punkt 145.B.205 ska ersättas med följande:

”145.B.205 Tilldelning av uppgifter”.

(iv) Följande rubrik ska införas efter rubrik 145.B.330:

”145.B.330A Ändringar av systemet för hantering av informationssäkerhet”.

(b) Efter punkt 145.A.200 ska följande punkt införas som punkt 145.A.200A:

”145.A.200A **System för hantering av informationssäkerhet**

Utöver det ledningssystem som avses i punkt 145.A.200 ska underhållsorganisationen inrätta, genomföra och upprätthålla ett system för hantering av informationssäkerhet i enlighet med genomförandeförordning (EU) 2023/203 för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten.”

(c) I punkt 145.B.125 ska följande punkt läggas till som punkt c:

”c) Medlemsstatens behöriga myndighet ska så snart som möjligt förse byrån med information av betydelse för säkerheten som härrör från de informationssäkerhetsrapporter som den har mottagit enligt punkt IS.I.OR.230 i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203.”

(d) Efter punkt 145.B.135 ska följande punkt införas som punkt 145.B.135A:

”145.B.135A **Omedelbar reaktion på en informationssäkerhetsincident eller sårbarhet med en inverkan på flygsäkerheten**

a) Den behöriga myndigheten ska införa ett system för att på lämpligt sätt samla in, analysera och sprida information om informationssäkerhetsincidenter och sårbarheter med en potentiell inverkan på flygsäkerheten som rapporteras av organisationer. Detta ska göras i samordning med andra relevanta myndigheter som ansvarar för informationssäkerhet eller cybersäkerhet i medlemsstaten för att öka samordningen av och förenligheten hos rapporteringssystemen.

b) Byrån ska införa ett system för att på lämpligt sätt analysera all relevant information av betydelse för säkerheten som mottagits i enlighet med punkt 145.B.125 c och utan onödigt dröjsmål förse medlemsstaterna och kommissionen med all information, inklusive rekommendationer eller korrigerande åtgärder som ska vidtas, som krävs för att de i god tid ska kunna reagera på en informationssäkerhetsincident eller sårbarhet med en potentiell inverkan på flygsäkerheten som inbegriper produkter, delar, utrustning som inte är fast installerad, personer eller organisationer som omfattas av förordning (EU) 2018/1139 och dess delegerade akter och genomförandeakter.

c) När den behöriga myndigheten har mottagit den information som avses i punkterna a och b ska den vidta lämpliga åtgärder för att ta itu med den potentiella inverkan av informationssäkerhetsincidenten eller sårbarheten på flygsäkerheten.

d) Åtgärder som vidtas i enlighet med punkt c ska omgående meddelas alla personer eller organisationer som ska följa dem enligt förordning (EU) 2018/1139 och dess delegerade akter och genomförandeakter. Medlemsstatens behöriga myndighet ska också informera byrån och, om kombinerade åtgärder krävs, de behöriga myndigheterna i övriga berörda medlemsstater, om dessa åtgärder."

(e) I punkt 145.B.200 ska följande punkt läggas till som punkt e:

"e) Utöver kraven i punkt a ska det ledningssystem som inrättats och upprätthålls av den behöriga myndigheten uppfylla kraven i bilaga I (Del-IS.AR) till genomförandeförordning (EU) 2023/203 för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten."

(f) Punkt 145.B.205 ska ändras på följande sätt:

(i) Rubriken ska ersättas med följande:

"145.B.205 **Tilldelning av uppgifter**".

(ii) Följande punkt ska läggas till som punkt c:

"c) När det gäller certifiering och tillsyn av organisationens efterlevnad av punkt 145.A.200A får den behöriga myndigheten tilldela uppgifter till behöriga organ i enlighet med punkt a eller till en relevant myndighet som ansvarar för informationssäkerhet eller cybersäkerhet i medlemsstaten. När den behöriga myndigheten tilldelar uppgifter ska den säkerställa att

1) alla aspekter som rör flygsäkerheten samordnas och beaktas av det behöriga organet eller den relevanta myndigheten,

2) resultaten av den certifiering och tillsyn som utförs av det behöriga organet eller den relevanta myndigheten integreras i den övergripande certifierings- och tillsynsdokumentationen för organisationen,

3) det egna systemet för hantering av informationssäkerhet, som inrättats i enlighet med punkt 145.B.200 e, omfattar alla arbetsuppgifter i samband med certifiering och fortlöpande tillsyn som utförs för dess räkning."

(g) I punkt 145.B.300 ska följande punkt läggas till som punkt g:

"g) När det gäller certifiering och tillsyn av organisationens efterlevnad av punkt 145.A.200A ska den behöriga myndigheten, utöver att uppfylla kraven i punkterna a–f, se över alla godkännanden som beviljats enligt punkt IS.I.OR.200 e i denna förordning eller punkt IS.D.OR.200 e i delegerad förordning (EU) 2022/1645 efter den tillämpliga tillsynscykeln och närhelst ändringar genomförs i organisationens arbetsområde."

(h) Efter punkt 145.B.330 ska följande punkt införas som punkt 145.B.330A:

"145.B.330A **Ändringar av systemet för hantering av informationssäkerhet**

a) För ändringar som hanteras och anmäls till den behöriga myndigheten i enlighet med förfarandet i punkt IS.I.OR.255 a i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203 ska den behöriga myndigheten inkludera en översyn av sådana ändringar i sin fortlöpande tillsyn i enlighet med principerna i punkt 145.B.300. Om bristande efterlevnad konstateras ska den behöriga myndigheten underrätta organisationen om detta, begära ytterligare ändringar och agera i enlighet med punkt 145.B.350.

b) För andra ändringar som kräver en ansökan om godkännande i enlighet med punkt IS.I.OR.255 b i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203 gäller följande:

1) När den behöriga myndigheten har mottagit ansökan om ändring ska den, innan den utfärdar ett godkännande, kontrollera att organisationen uppfyller de tillämpliga kraven.

2) Den behöriga myndigheten ska fastställa de villkor enligt vilka organisationen får verka under genomförandet av ändringen.

3) Efter att ha försäkrat sig om att organisationen uppfyller de tillämpliga kraven ska den behöriga myndigheten godkänna ändringen.”

(2) Bilaga III (Del-66) ska ändras på följande sätt:

(a) I innehållsförteckningen ska följande rubrik införas efter rubrik 66.B.10:

”66.B.15 System för hantering av informationssäkerhet”.

(b) Efter punkt 66.B.10 ska följande punkt införas som punkt 66.B.15:

”66.B.15 **System för hantering av informationssäkerhet**

Den behöriga myndigheten ska inrätta, genomföra och upprätthålla ett system för hantering av informationssäkerhet i enlighet med bilaga I (Del-IS.AR) till genomförandeförordning (EU) 2023/203 för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten.”

(3) Bilaga Vc (Del-CAMO) ska ändras på följande sätt:

(a) Innehållsförteckningen ska ändras på följande sätt:

(i) Följande rubrik ska införas efter rubrik CAMO.A.200:

”CAMO.A.200A System för hantering av informationssäkerhet”.

(ii) Följande rubrik ska införas efter rubrik CAMO.B.135:

”CAMO.B.135A Omedelbar reaktion på en informationssäkerhetsincident eller sårbarhet med en inverkan på flygsäkerheten”.

(iii) Rubriken till punkt CAMO.B.205 ska ersättas med följande:

”CAMO.B.205 Tilldelning av uppgifter”.

(iv) Följande rubrik ska införas efter rubrik CAMO.B.330:

”CAMO.B.330A Ändringar av systemet för hantering av informationssäkerhet”.

(b) Efter punkt CAMO.A.200 ska följande punkt införas som punkt CAMO.A.200A:

”CAMO.A.200A **System för hantering av informationssäkerhet**

Utöver det ledningssystem som avses i punkt CAMO.A.200 ska organisationen inrätta, genomföra och upprätthålla ett system för hantering av informationssäkerhet i enlighet med genomförandeförordning (EU) 2023/203 för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten.”

(c) I punkt CAMO.B.125 ska följande punkt läggas till som punkt c:

”c) Medlemsstatens behöriga myndighet ska så snart som möjligt förse byrån med information av betydelse för säkerheten som härrör från de informationssäkerhetsrapporter som den har mottagit enligt punkt IS.I.OR.230 i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203.”

(d) Efter punkt CAMO.B.135 ska följande punkt införas som punkt CAMO.B.135A:

”CAMO.B.135A **Omedelbar reaktion på en informationssäkerhetsincident eller sårbarhet med en inverkan på flygsäkerheten**

a) Den behöriga myndigheten ska införa ett system för att på lämpligt sätt samla in, analysera och sprida information om informationssäkerhetsincidenter och sårbarheter med en potentiell inverkan på flygsäkerheten som rapporteras av organisationer. Detta ska göras i samordning med andra relevanta myndigheter som ansvarar för informationssäkerhet eller cybersäkerhet i medlemsstaten för att öka samordningen av och förenligheten hos rapporteringssystemen.

b) Byrån ska införa ett system för att på lämpligt sätt analysera all relevant information av betydelse för säkerheten som mottagits i enlighet med punkt CAMO.B.125 c och utan onödigt dröjsmål förse medlemsstaterna och kommissionen med all information, inklusive rekommendationer eller korrigerande åtgärder som ska vidtas, som krävs för att de i god tid ska kunna reagera på en informationssäkerhetsincident eller sårbarhet med en potentiell inverkan på flygsäkerheten som inbegriper produkter, delar, utrustning som inte är fast installerad, personer eller organisationer som omfattas av förordning (EU) 2018/1139 och dess delegerade akter och genomförandeakter.

c) När den behöriga myndigheten har mottagit den information som avses i punkterna a och b ska den vidta lämpliga åtgärder för att ta itu med den potentiella inverkan av informationssäkerhetsincidenten eller sårbarheten på flygsäkerheten.

d) Åtgärder som vidtas i enlighet med punkt c ska omgående meddelas alla personer eller organisationer som ska följa dem enligt förordning (EU) 2018/1139 och dess delegerade akter och genomförandeakter. Medlemsstatens behöriga myndighet ska också informera byrån och, om kombinerade åtgärder krävs, de behöriga myndigheterna i övriga berörda medlemsstater, om dessa åtgärder.”

(e) I punkt CAMO.B.200 ska följande punkt läggas till som punkt e:

”e) Utöver kraven i punkt a ska det ledningssystem som inrättats och upprätthålls av den behöriga myndigheten uppfylla kraven i bilaga I (Del-IS.AR) till genomförandeförordning (EU) 2023/203 för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten.”

(f) Punkt CAMO.B.205 ska ändras på följande sätt:

i) Rubriken ska ersättas med följande:

”CAMO.B.205 **Tilldelning av uppgifter**”.

ii) Följande punkt ska läggas till som punkt c:

”c) När det gäller certifiering och tillsyn av organisationens efterlevnad av punkt CAMO.A.200A får den behöriga myndigheten tilldela uppgifter till behöriga organ i enlighet med punkt a eller till en relevant myndighet som ansvarar för informationssäkerhet eller cybersäkerhet i medlemsstaten. När den behöriga myndigheten tilldelar uppgifter ska den säkerställa att

1) alla aspekter som rör flygsäkerheten samordnas och beaktas av det behöriga organet eller den relevanta myndigheten,

2) resultaten av den certifiering och tillsyn som utförs av det behöriga organet eller den relevanta myndigheten integreras i den övergripande certifierings- och tillsynsdokumentationen för organisationen,

3) det egna systemet för hantering av informationssäkerhet, som inrättats i enlighet med punkt CAMO.B.200 e, omfattar alla arbetsuppgifter i samband med certifiering och fortlöpande tillsyn som utförs för dess räkning.”

(g) I punkt CAMO.B.300 ska följande punkt läggas till som punkt g:

”g) När det gäller certifiering och tillsyn av organisationens efterlevnad av punkt CAMO.A.200A ska den behöriga myndigheten, utöver att uppfylla kraven i punkterna a–f, se över alla godkännanden som beviljats enligt punkt IS.I.OR.200 e i denna förordning eller punkt IS.D.OR.200 e i delegerad förordning (EU) 2022/1645 efter den tillämpliga tillsynscykeln och närhelst ändringar genomförs i organisationens arbetsområde.”

(h) Efter punkt CAMO.B.330 ska följande punkt införas som punkt CAMO.B.330A:

”CAMO.B.330A **Ändringar av systemet för hantering av informationssäkerhet**

a) För ändringar som hanteras och anmäls till den behöriga myndigheten i enlighet med förfarandet i punkt IS.I.OR.255 a i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203 ska den behöriga myndigheten inkludera en översyn av sådana ändringar i sin fortlöpande tillsyn i enlighet med principerna i punkt CAMO.B.300. Om bristande efterlevnad konstateras ska den behöriga myndigheten underrätta organisationen om detta, begära ytterligare ändringar och agera i enlighet med punkt CAMO.B.350.

b) För andra ändringar som kräver en ansökan om godkännande i enlighet med punkt IS.I.OR.255 b i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203 gäller följande:

1) När den behöriga myndigheten har mottagit ansökan om ändring ska den, innan den utfärdar ett godkännande, kontrollera att organisationen uppfyller de tillämpliga kraven.

2) Den behöriga myndigheten ska fastställa de villkor enligt vilka organisationen får verka under genomförandet av ändringen.

3) Efter att ha försäkrat sig om att organisationen uppfyller de tillämpliga kraven ska den behöriga myndigheten godkänna ändringen.”

BILAGA VIII

Bilagorna II (Del-ATCO.AR) och III (Del-ATCO.OR) till förordning (EU) 2015/340 ska ändras på följande sätt:

(1) Bilaga II (Del-ATCO.AR) ska ändras på följande sätt:

(a) I punkt ATCO.AR.A.020 ska följande punkt läggas till som punkt c:

”c) Medlemsstatens behöriga myndighet ska så snart som möjligt förse byrån med information av betydelse för säkerheten som härrör från de informationssäkerhetsrapporter som den har mottagit enligt punkt IS.I.OR.230 i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203.”

(b) Efter punkt ATCO.AR.A.025 ska följande punkt införas som punkt ATCO.AR.A.025A:

”**ATCO.AR.A.025A Omedelbar reaktion på en informationssäkerhetsincident eller sårbarhet med en inverkan på flygsäkerheten**

a) Den behöriga myndigheten ska införa ett system för att på lämpligt sätt samla in, analysera och sprida information om informationssäkerhetsincidenter och sårbarheter med en potentiell inverkan på flygsäkerheten som rapporteras av organisationer. Detta ska göras i samordning med andra relevanta myndigheter som ansvarar för informationssäkerhet eller cybersäkerhet i medlemsstaten för att öka samordningen av och förenligheten hos rapporteringssystemen.

b) Byrån ska införa ett system för att på lämpligt sätt analysera all relevant information av betydelse för säkerheten som mottagits i enlighet med punkt ATCO.AR.A.020 och utan onödigt dröjsmål förse medlemsstaterna och kommissionen med all information, inklusive rekommendationer eller korrigerande åtgärder som ska vidtas, som krävs för att de i god tid ska kunna reagera på en informationssäkerhetsincident eller sårbarhet med en potentiell inverkan på flygsäkerheten som inbegriper produkter, delar, utrustning som inte är fast installerad, personer eller organisationer som omfattas av förordning (EU) 2018/1139 och dess delegerade akter och genomförandeakter.

c) När den behöriga myndigheten har mottagit den information som avses i punkterna a och b ska den vidta lämpliga åtgärder för att ta itu med den potentiella inverkan av informationssäkerhetsincidenten eller sårbarheten på flygsäkerheten.

d) Åtgärder som vidtas i enlighet med punkt c ska omgående meddelas alla personer eller organisationer som ska följa dem enligt förordning (EU) 2018/1139 och dess delegerade akter och genomförandeakter. Medlemsstatens behöriga myndighet ska också informera byrån och, om kombinerade åtgärder krävs, de behöriga myndigheterna i övriga berörda medlemsstater, om dessa åtgärder.”

(c) I punkt ATCO.AR.B.001 ska följande punkt läggas till som punkt e:

”e) Utöver kraven i punkt a ska det ledningssystem som inrättats och upprätthålls av den behöriga myndigheten uppfylla kraven i bilaga I (Del-IS.AR) till genomförandeförordning (EU) 2023/203 för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten.”

(d) Punkt ATCO.AR.B.005 ska ändras på följande sätt:

(i) Rubriken ska ersättas med följande:

”**ATCO.AR.B.005 Tilldelning av uppgifter**”.

(ii) Följande punkt ska läggas till som punkt c:

”c) När det gäller certifiering och tillsyn av organisationens efterlevnad av punkt ATCO.OR.C.001A får den behöriga myndigheten tilldela uppgifter till behöriga organ i enlighet med punkt a eller till en relevant myndighet som ansvarar för informationssäkerhet eller cybersäkerhet i medlemsstaten. När den behöriga myndigheten tilldelar uppgifter ska den säkerställa att

1) alla aspekter som rör flygsäkerheten samordnas och beaktas av det behöriga organet eller den relevanta myndigheten,

2) resultaten av den certifiering och tillsyn som utförs av det behöriga organet eller den relevanta myndigheten integreras i den övergripande certifierings- och tillsynsdokumentationen för organisationen,

3) det egna systemet för hantering av informationssäkerhet, som inrättats i enlighet med punkt ATCO.AR.B.001 e, omfattar alla arbetsuppgifter i samband med certifiering och fortlöpande tillsyn som utförs för dess räkning."

(e) I punkt ATCO.AR.C.001 ska följande punkt läggas till som punkt f:

"f) När det gäller certifiering och tillsyn av organisationens efterlevnad av punkt ATCO.OR.C.001A ska den behöriga myndigheten, utöver att uppfylla kraven i punkterna a–e, se över alla godkännanden som beviljats enligt punkt IS.I.OR.200 e i denna förordning eller punkt IS.D.OR.200 e i delegerad förordning (EU) 2022/1645 efter den tillämpliga tillsynscykeln och närhelst ändringar genomförs i organisationens arbetsområde."

(f) Efter punkt ATCO.AR.E.010 ska följande punkt införas som punkt ATCO.AR.E.010A:

"**ATCO.AR.E.010A Ändringar av systemet för hantering av informationssäkerhet**

a) För ändringar som hanteras och anmäls till den behöriga myndigheten i enlighet med förfarandet i punkt IS.I.OR.255 a i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203 ska den behöriga myndigheten inkludera en översyn av sådana ändringar i sin fortlöpande tillsyn i enlighet med principerna i punkt ATCO.AR.C.001. Om bristande efterlevnad konstateras ska den behöriga myndigheten underrätta organisationen om detta, begära ytterligare ändringar och agera i enlighet med punkt ATCO.AR.C.010.

b) För andra ändringar som kräver en ansökan om godkännande i enlighet med punkt IS.I.OR.255 b i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203 gäller följande:

1) När den behöriga myndigheten har mottagit ansökan om ändring ska den, innan den utfärdar ett godkännande, kontrollera att organisationen uppfyller de tillämpliga kraven.

2) Den behöriga myndigheten ska fastställa de villkor enligt vilka organisationen får verka under genomförandet av ändringen.

3) Efter att ha försäkrat sig om att organisationen uppfyller de tillämpliga kraven ska den behöriga myndigheten godkänna ändringen."

(2) Bilaga III (Del-ATCO.OR) ska ändras på följande sätt:

Efter punkt ATCO.OR.C.001 ska följande punkt införas som punkt ATCO.OR.C.001A:

"**ATCO.OR.C.001A System för hantering av informationssäkerhet**

Utöver det ledningssystem som avses i punkt ATCO.OR.C.001 ska utbildningsorganisationen inrätta, genomföra och upprätthålla ett system för hantering av informationssäkerhet i enlighet med genomförandeförordning (EU) 2023/203 för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten."

BILAGA IX

Bilagorna II (Del-ATM/ANS.AR) och III (Del-ATM/ANS.OR) till genomförandeförordning (EU) 2017/373 ska ändras på följande sätt:

(1) Bilaga II (Del-ATM/ANS.AR) ska ändras på följande sätt:

(a) I punkt ATM/ANS.AR.A.020 ska följande punkt läggas till som punkt c:

”c) Medlemsstatens behöriga myndighet ska så snart som möjligt förse byrån med information av betydelse för säkerheten som härrör från de informationssäkerhetsrapporter som den har mottagit enligt punkt IS.I.OR.230 i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203.”

(b) Efter punkt ATM/ANS.AR.A.025 ska följande punkt införas som punkt ATM/ANS.AR.A.025A:

”**ATM/ANS.AR.A.025A Omedelbar reaktion på en informationssäkerhetsincident eller sårbarhet med en inverkan på flygsäkerheten**

a) Den behöriga myndigheten ska införa ett system för att på lämpligt sätt samla in, analysera och sprida information om informationssäkerhetsincidenter och sårbarheter med en potentiell inverkan på flygsäkerheten som rapporteras av organisationer. Detta ska göras i samordning med andra relevanta myndigheter som ansvarar för informationssäkerhet eller cybersäkerhet i medlemsstaten för att öka samordningen av och förenligheten hos rapporteringssystemen.

b) Byrån ska införa ett system för att på lämpligt sätt analysera all relevant information av betydelse för säkerheten som mottagits i enlighet med punkt ATM/ANS.AR.A.020 c och utan onödigt dröjsmål förse medlemsstaterna och kommissionen med all information, inklusive rekommendationer eller korrigerande åtgärder som ska vidtas, som krävs för att de i god tid ska kunna reagera på en informationssäkerhetsincident eller sårbarhet med en potentiell inverkan på flygsäkerheten som inbegriper produkter, delar, utrustning som inte är fast installerad, personer eller organisationer som omfattas av förordning (EU) 2018/1139 och dess delegerade akter och genomförandeakter.

c) När den behöriga myndigheten har mottagit den information som avses i punkterna a och b ska den vidta lämpliga åtgärder för att ta itu med den potentiella inverkan av informationssäkerhetsincidenten eller sårbarheten på flygsäkerheten.

d) Åtgärder som vidtas i enlighet med punkt c ska omgående meddelas alla personer eller organisationer som ska följa dem enligt förordning (EU) 2018/1139 och dess delegerade akter och genomförandeakter. Medlemsstatens behöriga myndighet ska också informera byrån och, om kombinerade åtgärder krävs, de behöriga myndigheterna i övriga berörda medlemsstater, om dessa åtgärder.”

(c) I punkt ATM/ANS.AR.B.001 ska följande punkt läggas till som punkt e:

”e) Utöver kraven i punkt a ska det ledningssystem som inrättats och upprätthålls av den behöriga myndigheten uppfylla kraven i bilaga I (Del-IS.AR) till genomförandeförordning (EU) 2023/203 för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten.”

(d) Punkt ATM/ANS.AR.B.005 ska ändras på följande sätt:

i) Rubriken ska ersättas med följande:

”**ATM/ANS.AR.B.005 Tilldelning av uppgifter**”.

ii) Följande punkt ska läggas till som punkt c:

”c) När det gäller certifiering och tillsyn av organisationens efterlevnad av punkt ATM/ANS.OR.B.005A får den behöriga myndigheten tilldela uppgifter till behöriga organ i enlighet med punkt a eller till en relevant myndighet som ansvarar för informationssäkerhet eller cybersäkerhet i medlemsstaten. När den behöriga myndigheten tilldelar uppgifter ska den säkerställa att

1) alla aspekter som rör flygsäkerheten samordnas och beaktas av det behöriga organet eller den relevanta myndigheten,

2) resultaten av den certifiering och tillsyn som utförs av det behöriga organet eller den relevanta myndigheten integreras i den övergripande certifierings- och tillsynsdokumentationen för organisationen,

3) det egna systemet för hantering av informationssäkerhet, som inrättats i enlighet med punkt ATM/ANS.AR.B.001 e, omfattar alla arbetsuppgifter i samband med certifiering och fortlöpande tillsyn som utförs för dess räkning.”

(e) I punkt ATM/ANS.AR.C.010 ska följande punkt läggas till som punkt d:

”d) När det gäller certifiering och tillsyn av organisationens efterlevnad av punkt ATM/ANS.OR.B.005A ska den behöriga myndigheten, utöver att uppfylla kraven i punkterna a–c, se över alla godkännanden som beviljats enligt punkt IS.I.OR.200 e i denna förordning eller punkt IS.D.OR.200 e i delegerad förordning (EU) 2022/1645 efter den tillämpliga tillsynscykeln och närhelst ändringar genomförs i organisationens arbetsområde.”

(f) Efter punkt ATM/ANS.AR.C.025 ska följande punkt införas som punkt ATM/ANS.AR.C.025A:

”**ATM/ANS.AR.C.025A Ändringar av systemet för hantering av informationssäkerhet**

a) För ändringar som hanteras och anmäls till den behöriga myndigheten i enlighet med förfarandet i punkt IS.I.OR.255 a i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203 ska den behöriga myndigheten inkludera en översyn av sådana ändringar i sin fortlöpande tillsyn i enlighet med principerna i punkt ATM/ANS.AR.C.010. Om bristande efterlevnad konstateras ska den behöriga myndigheten underrätta organisationen om detta, begära ytterligare ändringar och agera i enlighet med punkt ATM/ANS.AR.C.050.

b) För andra ändringar som kräver en ansökan om godkännande i enlighet med punkt IS.I.OR.255 b i bilaga II (Del-IS.I.OR) till genomförandeförordning (EU) 2023/203 gäller följande:

1) När den behöriga myndigheten har mottagit ansökan om ändring ska den, innan den utfärdar ett godkännande, kontrollera att organisationen uppfyller de tillämpliga kraven.

2) Den behöriga myndigheten ska fastställa de villkor enligt vilka organisationen får verka under genomförandet av ändringen.

3) Efter att ha försäkrat sig om att organisationen uppfyller de tillämpliga kraven ska den behöriga myndigheten godkänna ändringen.”

(2) Bilaga III (Del-ATM/ANS.OR) ska ändras på följande sätt:

(a) Efter punkt ATM/ANS.OR.B.005 ska följande punkt införas som punkt ATM/ANS.OR.B.005A:

”**ATM/ANS.OR.B.005A System för hantering av informationssäkerhet**

Utöver det ledningssystem som avses i punkt ATM/ANS.OR.B.005 ska tjänsteleverantören inrätta, genomföra och upprätthålla ett system för hantering av informationssäkerhet i enlighet med genomförandeförordning (EU) 2023/203 för att säkerställa korrekt hantering av informationssäkerhetsrisker som kan påverka flygsäkerheten.”

(b) Punkt ATM/ANS.OR.D.010 ska ersättas med följande:

”**ATM/ANS.OR.D.010 Skyddsledning**

a) Leverantörer av flygtrafiktjänster och flödesplanering samt nätverksförvaltaren ska, som en integrerad del av sitt ledningssystem enligt krav i punkt ATM/ANS.OR.B.005, inrätta ett skyddsledningssystem för att säkerställa

1) skyddet av anläggningen och personalen för att förhindra att brottsliga handlingar stör tillhandahållandet av tjänster,

2) skyddet mot obehörig åtkomst av operativa data som leverantörerna tar emot eller tar fram eller använder på annat sätt, så att endast de som är bemyndigade kommer åt dessa data.

b) Skyddsledningssystemet ska fastställa

1) processer och förfaranden för bedömning och reducering av skyddsrisker, övervakning och höjning av skyddet, skyddsöversyn och spridning av erfarenheter,

2) medel för att identifiera, övervaka och upptäcka brister i skyddet och för att varsko personalen på lämpligt sätt,

3) medel för att kontrollera följderna av brister i skyddet och för att identifiera återhämtnings- och motåtgärder i syfte att förhindra en upprepning.

c) Leverantörer av flygtrafiktjänster och flödesplanering samt nätverksförvaltaren ska säkerställa säkerhetsprövningen av sin personal, om så är lämpligt, och samordna med civila och militära myndigheter för att säkerställa att deras anläggningar, personal och data är skyddade.

d) De aspekter som rör informationssäkerhet ska hanteras i enlighet med punkt ATM/ANS.OR.B.005A.”