GEDELEGEERDE VERORDENING (EU) 2022/1645 VAN DE COMMISSIE

van 14 juli 2022

tot vaststelling van regels voor de toepassing van Verordening (EU) 2018/1139 van het Europees Parlement en de Raad, wat betreft eisen voor het beheer van risico's voor de informatiebeveiliging met mogelijke gevolgen voor de luchtvaartveiligheid voor organisaties die onder Verordeningen (EU) nr. 748/2012 en (EU) nr. 139/2014 van de Commissie vallen en tot wijziging van Verordeningen (EU) nr. 748/2012 en (EU) nr. 139/2014 van de Commissie

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2018/1139 van het Europees Parlement en de Raad van 4 juli 2018 inzake gemeenschappelijke regels op het gebied van burgerluchtvaart en tot oprichting van een Agentschap van de Europese Unie voor de veiligheid van de luchtvaart, en tot wijziging van de Verordeningen (EG) nr. 2111/2005, (EG) nr. 1008/2008, (EU) nr. 996/2010, (EU) nr. 376/2014 en de Richtlijnen 2014/30/EU en 2014/53/EU van het Europees Parlement en de Raad, en tot intrekking van de Verordeningen (EG) nr. 552/2004 en (EG) nr. 216/2008 van het Europees Parlement en de Raad en Verordening (EEG) nr. 3922/91 van de Raad ([1]), en met name artikel 19, lid 1, punt g), en artikel 39, lid 1, punt b).

Overwegende hetgeen volgt:

(1) Overeenkomstig de essentiële eisen van punt 3.1, b), bij bijlage II van Verordening (EU) 2018/1139 moeten ontwerp- en productieorganisaties een beheersysteem opzetten en onderhouden om veiligheidsrisico's te beheren.

(2) Overeenkomstig de essentiële eisen van punten 2.2.1 en 5.2 van bijlage VII bij Verordening (EU) 2018/1139 moeten exploitanten van luchtvaartterreinen en organisaties die verantwoordelijk zijn voor het verlenen van platformbeheersdiensten, bovendien een beheersysteem opzetten en onderhouden om veiligheidsrisico's te beheren.

(3) De in overwegingen 1 en 2 bedoelde veiligheidsrisico's kunnen voortvloeien uit verschillende bronnen, met inbegrip van ontwerp- en onderhoudsgebreken, aspecten van menselijke prestaties, milieubedreigingen en bedreigingen voor de informatiebeveiliging. De beheersystemen die worden toegepast door de in overwegingen 1 en 2 genoemde organisaties moeten daarom niet alleen rekening houden met veiligheidsrisico's die voortvloeien uit toevallige gebeurtenissen, maar ook met veiligheidsrisico's die voortvloeien uit bedreigingen voor de informatiebeveiliging waarbij bestaande tekortkomingen kunnen worden uitgebuit door personen met kwaadwillige bedoelingen. Die risico's voor de informatiebeveiliging in de burgerluchtvaart nemen voortdurend toe omdat de actuele informatiesystemen steeds meer met elkaar verweven zijn en steeds vaker het doelwit worden van kwaadwillige actoren.

(4) De risico's in verband met die informatiesystemen blijven niet beperkt tot mogelijke aanvallen op de cyberruimte, maar omvatten ook bedreigingen die van invloed kunnen zijn op processen en procedures en op de prestaties van mensen.

(5) Een aanzienlijk aantal organisaties maakt reeds gebruik van internationale normen, zoals ISO 27001, om digitale informatie en gegevens te beveiligen. Het is mogelijk dat deze normen niet volledig beantwoorden aan alle specifieke kenmerken van de burgerluchtvaart.

(6) Het is dan ook passend eisen in te voeren voor het beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.

(7) Het is van essentieel belang dat deze eisen betrekking hebben op de verschillende luchtvaartdomeinen en hun interfaces aangezien de luchtvaart een sterk onderling verweven systeem is. Ze moeten dan ook van toepassing zijn op alle organisatie die reeds over een beheersysteem moeten beschikken overeenkomstig de bestaande luchtvaartveiligheidswetgeving van de Unie.

(8) De in deze verordening vastgestelde eisen moeten consequent worden toegepast op alle luchtvaartdomeinen en tegelijkertijd zo weinig mogelijk gevolgen hebben voor de luchtvaartveiligheidswetgeving van de Unie die reeds van toepassing is op deze domeinen.

([1]) PB L 212 van 22.8.2018, blz. 1.

(9) De in deze verordening vastgestelde eisen mogen geen afbreuk doen aan de eisen inzake informatiebeveiliging en cyberbeveiliging die zijn vastgesteld in punt 1.7 van de bijlage bij Uitvoeringsverordening (EU) 2015/1998 van de Commissie ([2]) en in artikel 14 van Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad ([3]).

(10) De definitie van informatiebeveiliging die in deze rechtshandeling wordt gebruikt, mag niet worden geïnterpreteerd als een afwijking van de definitie van beveiliging van netwerk- en informatiesystemen in Richtlijn (EU) 2016/1148.

(11) Indien onder deze verordening vallende organisaties reeds onderworpen zijn aan beveiligingseisen die voortvloeien uit andere in overweging 9 bedoelde rechtshandelingen van de Unie die qua werking gelijkwaardig zijn aan de in deze verordening vastgestelde voorschriften, moet de naleving van die beveiligingseisen worden beschouwd als naleving van de in deze verordening vastgestelde eisen, teneinde verdubbeling van wettelijke voorschriften te vermijden.

(12) Onder deze verordening vallende organisaties die reeds onderworpen zijn aan beveiligingseisen die voortvloeien uit Uitvoeringsverordening (EU) 2015/1998, moeten ook voldoen aan de eisen van bijlage I (Deel IS.D.OR.230 "Regeling voor de externe rapportering van informatiebeveiligingsincidenten") bij deze verordening aangezien Uitvoeringsverordening (EU) 2015/1998 geen bepalingen bevat die betrekking hebben op de externe rapportering van informatiebeveiligingsincidenten.

(13) Verordeningen (EU) nr. 748/2012 ([4]) en (EU) nr. 139/2014 ([5]) van de Commissie moeten worden gewijzigd om het verband te leggen tussen de in de bovengenoemde verordeningen voorgeschreven beheersystemen en de in deze verordening voorgeschreven eisen inzake het beheer van informatiebeveiliging.

(14) Om organisaties voldoende tijd te geven om de naleving van de bij deze verordening ingevoerde nieuwe regels en procedures te waarborgen, moet deze verordening van toepassing worden met ingang van drie jaar na de datum van inwerkingtreding.

(15) De in deze verordening vastgestelde eisen zijn gebaseerd op Advies nr. 03/2021 ([6]), dat door het Agentschap is uitgebracht overeenkomstig artikel 75, lid 2, punten b) en c), en artikel 76, lid 1, van Verordening (EU) 2018/1139.

(16) Overeenkomstig artikel 128, lid 4, van Verordening (EU) 2018/1139, heeft de Commissie de door elke lidstaat aangewezen deskundigen geraadpleegd overeenkomstig de beginselen die zijn neergelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven ([7]),

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Onderwerp

In deze verordening worden de eisen vastgesteld waaraan de in artikel 2 bedoelde organisaties moeten voldoen om informatiebeveiligingsrisico's met potentiële gevolgen voor de luchtvaartveiligheid, die informatie- en communicatietechnologiesystemen en voor burgerluchtvaartdoeleinden gebruikte gegevens kunnen aantasten, op te sporen en te beheren en om informatiebeveiligingsvoorvallen op te sporen, om te bepalen welke daarvan worden beschouwd als informatiebeveiligingsincidenten met potentiële gevolgen voor de luchtvaartveiligheid, en om te reageren op en te herstellen van dergelijke informatiebeveiligingsincidenten.

([2]) Uitvoeringsverordening (EU) 2015/1998 van de Commissie van 5 november 2015 tot vaststelling van gedetailleerde maatregelen voor de tenuitvoerlegging van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart (PB L 299 van 14.11.2015, blz. 1).

([3]) Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016, blz. 1).

([4]) Verordening (EU) nr. 748/2012 van de Commissie van 3 augustus 2012 tot vaststelling van uitvoeringsvoorschriften inzake de luchtwaardigheid en milieucertificering van luchtvaartuigen en aanverwante producten, onderdelen en uitrustingsstukken, alsmede voor de certificering van ontwerp- en productieorganisaties (PB L 224 van 21.8.2012, blz. 1).

([5]) Verordening (EU) nr. 139/2014 van de Commissie van 12 februari 2014 tot vaststelling van eisen en administratieve procedures met betrekking tot luchtvaartterreinen, overeenkomstig Verordening (EG) nr. 216/2008 van het Europees Parlement en de Raad (PB L 44 van 14.2.2014, blz. 1).

([6]) https://www.easa.europa.eu/document-library/opinions

([7]) PB L 123 van 12.5.2016, blz. 1.

Artikel 2

Toepassingsgebied

1. Deze verordening is van toepassing op de volgende organisaties:

a) productieorganisaties en ontwerporganisaties die onderworpen zijn aan subdelen G en J van sectie A van bijlage I (deel 21) bij Verordening (EU) nr. 748/2012, behalve productieorganisaties en ontwerporganisaties die uitsluitend betrokken zijn bij het ontwerp en/of de productie van ELA2-luchtvaartuigen zoals gedefinieerd in artikel 1, lid 2, punt j), van Verordening (EU) nr. 748/2012;

b) exploitanten van luchtvaartterreinen en verleners van platformbeheerdiensten die onderworpen zijn aan bijlage III "Deel organisatievereisten (Deel-ADR.OR)" bij Verordening (EU) nr. 139/2014.

2. Deze verordening doet geen afbreuk aan de eisen inzake informatiebeveiliging en cyberbeveiliging die zijn vastgesteld in punt 1.7 van de bijlage bij Uitvoeringsverordening (EU) 2015/1998 en in artikel 14 van Richtlijn (EU) 2016/1148.

Artikel 3

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

1) "informatiebeveiliging": de instandhouding van de vertrouwelijkheid, integriteit, authenticiteit en beschikbaarheid van netwerk- en informatiesystemen;

2) "informatiebeveiligingsvoorval": een vastgestelde toestand van een systeem, dienst of netwerk die wijst op een mogelijke inbreuk op het informatiebeveiligingsbeleid of een storing van de informatiebeveiligingscontroles, of een voorheen onbekende situatie die relevant kan zijn voor de informatiebeveiliging;

3) "incident": een gebeurtenis die een negatief effect heeft op de beveiliging van netwerk- en informatiesystemen, zoals gedefinieerd in artikel 4, punt 7, van Richtlijn (EU) 2016/1148;

4) "informatiebeveiligingsrisico": het risico voor organisatorische burgerluchtvaartactiviteiten, activa, individuen en andere organisaties als gevolg van het potentieel van een informatiebeveiligingsvoorval. Informatiebeveiligingsrisico's houden verband met de mogelijkheid dat bedreigingen gebruikmaken van kwetsbaarheden van een informatiebron of groep van informatieactiva;

5) "bedreiging": een potentiële inbreuk op de informatiebeveiliging die bestaat wanneer er sprake is van een entiteit, omstandigheid, actie of gebeurtenis die schade kan veroorzaken;

6) "kwetsbaarheid": een tekortkoming of zwak punt in een activum of een systeem, procedures, ontwerp, toepassing, of informatiebeveiligingsmaatregelen die kunnen worden misbruikt en leiden tot een inbreuk op of schending van het informatiebeveiligingsbeleid.

Artikel 4

Eisen die voortvloeien uit andere wetgeving van de Unie

1. Wanneer een in artikel 2 bedoelde organisatie voldoet aan de in artikel 14 van Richtlijn (EU) 2016/1148 vastgestelde beveiligingseisen die gelijkwaardig zijn aan de in deze verordening vastgestelde eisen, wordt de naleving van die beveiligingseisen beschouwd als naleving van de in deze verordening vastgestelde eisen.

2. Wanneer een in artikel 2 bedoelde organisatie een exploitant of entiteit is als bedoeld in de overeenkomstig artikel 10 van Verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad ([8]) opgestelde nationale programma's voor de beveiliging van de burgerluchtvaart van de lidstaten, worden de cyberbeveiligingseisen in punt 1.7 van de bijlage bij Uitvoeringsverordening (EU) 2015/1998 als gelijkwaardig beschouwd aan de in deze verordening vastgestelde eisen, behalve wat betreft punt IS.D.OR.230 van de bijlage bij deze verordening, dat moet worden nageleefd.

([8]) Verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad van 11 maart 2008 inzake gemeenschappelijke regels op het gebied van de beveiliging van de burgerluchtvaart en tot intrekking van Verordening (EG) nr. 2320/2002 (PB L 97 van 9.4.2008, blz. 72);

3. Na raadpleging van het EASA en de in artikel 11 van Richtlijn (EU) 2016/1148 bedoelde samenwerkingsgroep kan de Commissie richtsnoeren uitvaardigen voor de beoordeling van de gelijkwaardigheid van de in deze verordening en Richtlijn (EU) 2016/1148 vastgestelde eisen.

Artikel 5

Bevoegde autoriteit

1. De autoriteit die verantwoordelijk is voor certificering en toezicht op de naleving van deze verordening is:

a) met betrekking tot de in artikel 2, punt a), bedoelde organisaties, de bevoegde autoriteit die is aangewezen overeenkomstig bijlage I (deel 21) bij Verordening (EU) nr. 748/2012;

b) met betrekking tot de in artikel 2, punt b), bedoelde organisaties, de bevoegde autoriteit die is aangewezen overeenkomstig bijlage III (deel-ADR.OR) bij Verordening (EU) nr. 139/2014.

2. Met het oog op de toepassing van deze verordening mogen de lidstaten een onafhankelijke en zelfstandige entiteit aanwijzen, die de rol en verantwoordelijkheden opneemt van de in lid 1 bedoelde bevoegde autoriteit. In dat geval worden maatregelen getroffen voor coördinatie tussen die entiteit en de in lid 1 bevoegde autoriteiten, teneinde te garanderen dat de organisatie doeltreffend toezicht houdt op alle eisen waaraan moet worden voldaan.

Artikel 6

Wijziging van Verordening (EU) nr. 748/2012

Bijlage I (deel 21) bij Verordening (EU) nr. 748/2012 wordt als volgt gewijzigd:

1) De inhoudsopgave wordt als volgt gewijzigd:

   a) na 21.A.139 wordt de volgende titel ingevoegd:

   "**21.A.139A Beheersysteem voor informatiebeveiliging**";

   b) na 21.A.239 wordt de volgende titel ingevoegd:

   "**21.A.239A Beheersysteem voor informatiebeveiliging**".

2) Na punt 21.A.139 wordt het volgende punt 21.A.139A ingevoegd:

"**21.A.139A Beheersysteem voor informatiebeveiliging**

Naast het bij punt 21.A.139 vereiste productiebeheersysteem moet de productieorganisatie een beheersysteem voor informatiebeveiliging opzetten, toepassen en onderhouden overeenkomstig Gedelegeerde Verordening (EU) 2022/1645 van de Commissie (*) om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.

(*) Gedelegeerde Verordening (EU) 2022/1645 van de Commissie van 14 juli 2022 tot vaststelling van regels voor de toepassing van Verordening (EU) 2018/1139 van het Europees Parlement en de Raad, wat betreft eisen voor het beheer van risico's voor de informatiebeveiliging met mogelijke gevolgen voor de luchtvaartveiligheid voor organisaties die onder Verordeningen (EU) nr. 748/2012 en (EU) nr. 139/2014 van de Commissie vallen en tot wijziging van Verordeningen (EU) nr. 748/2012 en (EU) nr. 139/2014 van de Commissie (PB L 248 van 26.9.2022, blz. 18).".

3) Na punt 21.A.239 wordt het volgende punt 21.A.239A ingevoegd:

"**21.A.239A Beheersysteem voor informatiebeveiliging**

Naast het bij punt 21.A.239 vereiste ontwerpbeheersysteem moet de ontwerporganisatie een beheersysteem voor informatiebeveiliging opzetten, toepassen en onderhouden overeenkomstig Gedelegeerde Verordening (EU) 2022/1645 om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.".

Artikel 7

Wijziging van Verordening (EU) nr. 139/2014

Bijlage III (Deel-ADR.OR) bij Verordening (EU) nr. 139/2014 wordt als volgt gewijzigd:

1) Na punt ADR.OR.D.005 wordt het volgende punt ADR.OR.D.005A ingevoegd:

"**ADR.OR.D.005A Beheersysteem voor informatiebeveiliging**

De exploitant van het luchtvaartterrein ontwikkelt, implementeert en onderhoudt een beheersysteem voor informatiebeveiliging overeenkomstig Gedelegeerde Verordening (EU) 2022/1645 van de Commissie (*) om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.

(*) Gedelegeerde Verordening (EU) 2022/1645 van de Commissie van 14 juli 2022 tot vaststelling van regels voor de toepassing van Verordening (EU) 2018/1139 van het Europees Parlement en de Raad, wat betreft eisen voor het beheer van risico's voor de informatiebeveiliging met mogelijke gevolgen voor de luchtvaartveiligheid voor organisaties die onder Verordeningen (EU) nr. 748/2012 en (EU) nr. 139/2014 van de Commissie vallen en tot wijziging van Verordeningen (EU) nr. 748/2012 en (EU) nr. 139/2014 van de Commissie (PB L 248 van 26.9.2022, blz. 18).".

2) Punt ADR.OR.D.007 wordt vervangen door:

"**ADR.OR.D.007 Beheer van luchtvaartgegevens en luchtvaartinformatie**

a) Als onderdeel van zijn beheersysteem, zorgt de exploitant van het luchtvaartterrein voor de toepassing en actualisering van een kwaliteitsbeheersysteem met betrekking tot:

   1) zijn activiteiten met betrekking tot luchtvaartgegevens;

   2) zijn activiteiten met betrekking tot het verstrekken van luchtvaartinformatie.

b) In het kader van zijn beheersysteem dient de exploitant van het luchtvaartterrein een beveiligingsbeheersysteem op te zetten om de vluchtuitvoeringsgegevens die hij ontvangt, produceert of anderszins gebruikt te beveiligen en aldus te garanderen dat die gegevens uitsluitend toegankelijk zijn voor daartoe gemachtigde personen.

c) In het beveiligingsbeheersysteem worden de volgende elementen gedefinieerd:

   1) de procedures voor de beoordeling en beperking van risico's op het gebied van de beveiliging van gegevens, het toezicht op en de verhoging van de beveiliging, de evaluatie van de beveiliging en de verspreiding van opgedane ervaringen;

   2) de methoden die zijn ontworpen om lekken in de beveiliging op te sporen en het personeel op passende wijze te waarschuwen;

   3) de methoden om de gevolgen van schendingen van de beveiliging onder controle te houden en om herstel- en schadebeperkingsprocedures vast te stellen teneinde herhaling te voorkomen.

d) De exploitant van het luchtvaartterrein zorgt ervoor dat zijn personeel over een veiligheidsmachtiging beschikt met betrekking tot de beveiliging van luchtvaartgegevens.

e) De aspecten die verband houden met informatiebeveiliging worden beheerd overeenkomstig punt ADR.OR.D.005A.".

3) Na punt ADR.OR.F.045 wordt het volgende punt ADR.OR.F.045A ingevoegd:

"**ADR.OR.F.045A Beheersysteem voor informatiebeveiliging**

De organisatie die verantwoordelijk is voor de verlening platformbeheerdiensten ontwikkelt, implementeert en onderhoudt een beheersysteem voor informatiebeveiliging overeenkomstig Gedelegeerde Verordening (EU) 2022/1645 om te zorgen voor een goed beheer van risico's voor de informatiebeveiliging die gevolgen kunnen hebben voor de veiligheid van de luchtvaart.".

Artikel 8

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Zij is van toepassing met ingang van 16 oktober 2025.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 14 juli 2022.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

BIJLAGE

INFORMATIEBEVEILIGING — VEREISTEN VAN DE ORGANISATIE

[PART-IS.D.OR]

IS.D.OR.100 Toepassingsgebied

IS.D.OR.200 Beheersysteem voor informatiebeveiliging

IS.D.OR.205 Beoordeling van risico's voor de informatiebeveiliging

IS.D.OR.210 Behandeling van risico's voor de informatiebeveiliging

IS.D.OR.215 Regeling voor interne rapportage over informatiebeveiliging

IS.D.OR.220 Informatiebeveiligingsincidenten — opsporing, reactie en herstel

IS.D.OR.225 Reactie op door de bevoegde autoriteit gemelde bevindingen

IS.D.OR.230 Regeling voor externe rapportage over informatiebeveiliging

IS.D.OR.235 Uitbesteding van activiteiten op het gebied van informatiebeveiligingsbeheer

IS.D.OR.240 Eisen met betrekking tot personeel

IS.D.OR.245 Bijhouden van gegevens

IS.D.OR.250 Handboek informatiebeveiligingsbeheer

IS.D.OR.255 Wijzigingen van het beheersysteem voor informatiebeveiliging

IS.D.OR.260 Permanente verbetering

IS.D.OR.100 Toepassingsgebied

In dit deel worden de eisen vastgesteld waaraan de in artikel 2 van deze verordening bedoelde organisaties moeten voldoen.

IS.D.OR.200 Beheersysteem voor informatiebeveiliging

a) Om de in artikel 1 uiteengezette doelstellingen te verwezenlijken, ontwikkelt, implementeert en onderhoudt de organisatie een beheersysteem voor informatiebeveiliging, dat waarborgt dat de organisatie:

1) een beleid inzake informatiebeveiliging vaststelt, waarin de algemene beginselen van de organisatie met betrekking tot de mogelijke gevolgen van informatiebeveiligingsrisico's voor de veiligheid van de luchtvaart worden uiteengezet;

2) informatiebeveiligingsrisico's vaststelt en beoordeelt overeenkomstig IS.D.OR.205;

3) maatregelen voor de behandeling van informatiebeveiligingsrisico's definieert en uitvoert overeenkomstig IS.D.OR.210;

4) een regeling voor interne rapportage over informatiebeveiliging toepast overeenkomstig IS.D.OR.215;

5) overeenkomstig IS.D.OR.220 de maatregelen vaststelt en toepast die nodig zijn om informatiebeveiligingsvoorvallen op te sporen, om te bepalen welke daarvan worden beschouwd als informatiebeveiligingsincidenten met potentiële gevolgen voor de luchtvaartveiligheid, met uitzondering van de voorvallen die zijn toegestaan uit hoofde van IS.D.OR.205, punt e), en om te reageren op en te herstellen van dergelijke informatiebeveiligingsincidenten;

6) de maatregelen uitvoert die door de bevoegde autoriteit zijn gemeld als een onmiddellijke reactie op een informatiebeveiligingsincident of kwetsbaarheid met gevolgen voor de veiligheid van de luchtvaart;

7) passende maatregelen neemt, overeenkomstig IS.D.OR.225, om de door de bevoegde autoriteit gemelde bevindingen aan te pakken;

8) een extern rapportagesysteem toepast, overeenkomstig IS.D.OR.230, om de bevoegde autoriteit in staat te stellen passende maatregelen te nemen;

9) voldoet aan de eisen van IS.D.OR.235 bij het uitbesteden van een deel van de in IS.D.OR.200 bedoelde activiteiten aan andere organisaties;

10) voldoet aan de personeelseisen die zijn vastgesteld in IS.D.OR.240;

11) voldoet aan de eisen inzake het bijhouden van gegevens die zijn vastgesteld in IS.D.OR.245;

12) toezicht houdt op de naleving door de organisatie van de eisen van deze verordening en feedback over bevindingen verstrekt aan de verantwoordelijke manager of, in het geval van ontwerporganisaties, aan het ontwerphoofd van de organisatie, teneinde ervoor te zorgen dat de corrigerende maatregelen doeltreffend worden uitgevoerd;

13) beschermt, onverminderd de toepasselijke vereisten inzake rapportage van incidenten, de vertrouwelijkheid van alle informatie die de organisatie heeft ontvangen van andere organisaties, volgens het niveau van vertrouwelijkheid.

b) Om blijvend te voldoen aan de in artikel 1 vermelde eisen, voert de organisatie een continu verbeteringsproces uit overeenkomstig IS.D.OR.260.

c) Overeenkomstig IS.D.OR.250 documenteert de organisatie alle belangrijke processen, procedures, rollen en verantwoordelijkheden die vereist zijn om te voldoen aan IS.D.OR.200, punt a), en stelt zij een procedure vast voor het wijzigen van die documentatie. Wijzigingen van die processen, procedures, rollen en verantwoordelijkheden worden beheerd overeenkomstig IS.D.OR.255.

d) De processen, procedures, rollen en verantwoordelijkheden die door de organisatie zijn vastgesteld om te voldoen aan punt IS.D.OR.200, punt a), moeten overeenstemmen met de aard en complexiteit van haar activiteiten, op basis van een beoordeling van de aan die activiteiten inherente risico's voor de informatiebeveiliging, en mogen worden geïntegreerd in andere bestaande beheersystemen die reeds door de organisatie worden toegepast.

e) Onverminderd de verplichting om te voldoen aan de rapportagevereisten van Verordening (EU) nr. 376/2014 van het Europees Parlement en de Raad [1] en de eisen van IS.D.OR.200, punt a), 13), kan de organisatie toestemming krijgen van de bevoegde autoriteit om de in de punten a) tot en met d) bedoelde eisen en de aanverwante eisen in IS.D.OR.205 tot en met IS.D.OR.260 niet toe te passen, als zij tot tevredenheid van die autoriteit aantoont dat haar activiteiten, faciliteiten en middelen, alsook de diensten die zij exploiteert, verleent, ontvangt en onderhoudt, geen informatiebeveiligingsrisico's met mogelijke gevolgen voor de veiligheid van de luchtvaart inhouden, noch voor haarzelf, noch voor andere organisaties. De toestemming wordt gebaseerd op een gedocumenteerde beoordeling van de informatiebeveiligingsrisico's die door de organisatie of door een derde partij wordt uitgevoerd overeenkomstig IS.D.OR.205 en door haar bevoegde autoriteit wordt beoordeeld en goedgekeurd.

De blijvende geldigheid van die toestemming zal door de bevoegde autoriteit worden beoordeeld na de toepasselijke auditcyclus en telkens wanneer wijzigingen worden doorgevoerd in het toepassingsgebied van de werkzaamheden van de organisatie.

IS.D.OR.205 Beoordeling van risico's voor de informatiebeveiliging

a) De organisatie identificeert al haar elementen die kunnen worden blootgesteld aan informatiebeveiligingsrisico's, waaronder:

1) de activiteiten, faciliteiten en middelen van de organisatie, en de diensten die de organisatie exploiteert, verleent, ontvangt of onderhoudt;

2) de apparatuur, systemen, gegevens en informatie die bijdragen tot de werking van de in punt 1) vermelde elementen.

b) De organisatie identificeert de interfaces die zij heeft met andere organisaties en die kunnen leiden tot wederzijdse blootstelling aan informatiebeveiligingsrisico's.

c) Met betrekking tot de in de punten a) en b) vermelde elementen en interfaces identificeert de organisatie de informatiebeveiligingsrisico's die gevolgen kunnen hebben voor de veiligheid van de luchtvaart. Voor elk geïdentificeerd risico moet de organisatie:

1) een risiconiveau toekennen op basis van een classificatie die zij vooraf heeft opgesteld;

[1] Verordening (EU) nr. 376/2014 van het Europees Parlement en de Raad van 3 april 2014 inzake het melden, onderzoeken en opvolgen van voorvallen in de burgerluchtvaart en tot wijziging van Verordening (EU) nr. 996/2010 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2003/42/EG van het Europees Parlement en de Raad en de Verordeningen (EG) nr. 1321/2007 en (EG) nr. 1330/2007 van de Commissie (PB L 122 van 24.4.2014, blz. 18).

2) elk risico en het niveau ervan koppelen aan het overeenkomstige element of de overeenkomstige interface, zoals vastgesteld overeenkomstig de punten a) en b).

De in punt 1) bedoelde vooraf opgestelde classificatie houdt rekening met de mogelijkheid dat het dreigingsscenario zich voordoet en met de ernst van de gevolgen daarvan voor de veiligheid. Op basis van die classificatie en rekening houdend met de vraag of de organisatie beschikt over een gestructureerd en aanvaardbaar proces voor het beheer van de risico's van haar activiteiten, moet de organisatie in staat zijn te bepalen of het risico aanvaardbaar is of moet worden behandeld overeenkomstig IS.D.OR.210.

Om risicobeoordelingen gemakkelijker te kunnen vergelijken, moet bij de toekenning van het risiconiveau overeenkomstig punt 1) rekening worden gehouden met relevante informatie die in overleg met de in punt b) bedoelde organisaties is verkregen.

d) De organisatie evalueert en actualiseert de overeenkomstig de punten a), b) en c) uitgevoerde risicobeoordeling in elk van de volgende situaties:

1) er is een wijziging in de elementen die onderhevig zijn aan informatiebeveiligingsrisico's;

2) er is een wijziging in de interfaces tussen de organisatie en andere organisaties, of in de risico's die door de andere organisaties zijn meegedeeld;

3) er is een wijziging in de informatie of kennis die gebruikt is voor de identificatie, analyse en classificatie van risico's;

4) er zijn lessen getrokken uit de analyse van informatiebeveiligingsincidenten.

IS.D.OR.210 Behandeling van risico's voor de informatiebeveiliging

a) De organisatie ontwikkelt maatregelen om onaanvaardbare risico's aan te pakken die overeenkomstig IS.D.OR.205 zijn vastgesteld, voert deze maatregelen tijdig uit en controleert de blijvende doeltreffendheid ervan. Die maatregelen moeten de organisatie in staat stellen om:

1) controle uit te oefenen op de omstandigheden die ertoe bijdragen dat het dreigingsscenario zich effectief voordoet;

2) de gevolgen van het dreigingsscenario voor de veiligheid van de luchtvaart te beperken;

3) de risico's te vermijden.

Deze maatregelen mogen niet leiden tot nieuwe potentiële onaanvaardbare risico's voor de veiligheid van de luchtvaart.

b) De in IS.D.OR.240, punten a) en b), bedoelde persoon en andere betrokken personeelsleden van de organisatie worden in kennis gesteld van de resultaten van de overeenkomstig IS.D.OR.205 uitgevoerde risicobeoordeling, de overeenkomstige dreigingsscenario's en de uit te voeren maatregelen.

De organisatie stelt de organisaties waarmee zij een interface heeft overeenkomstig IS.D.OR.205, punt b), eveneens in kennis van elk risico dat door beide organisaties wordt gedeeld.

IS.D.OR.215 Regeling voor interne rapportage over informatiebeveiliging

a) De organisatie zet een interne rapportageregeling op om het mogelijk te maken informatiebeveiligingsvoorvallen te verzamelen en te beoordelen, met inbegrip van die welke overeenkomstig IS.D.OR.230 moeten worden gerapporteerd.

b) Die regeling en het in IS.D.OR.220 bedoelde proces moeten de organisatie in staat stellen om:

1) te bepalen welke van de overeenkomstig punt a) gemelde gebeurtenissen moeten worden beschouwd als informatiebeveiligingsincidenten of kwetsbaarheden met potentiële gevolgen voor de veiligheid van de luchtvaart;

2) de oorzaken van en de factoren die bijdragen tot de overeenkomstig punt 1) vastgestelde incidenten en kwetsbaarheden bepalen en aanpakken in het kader van het proces voor het beheer van risico's voor de informatiebeveiliging, overeenkomstig IS.D.OR.205 en IS.D.OR.220;

3) erop toezien dat een evaluatie wordt uitgevoerd van alle bekende relevante informatie met betrekking tot de overeenkomstig punt 1) vastgestelde informatiebeveiligingsincidenten en kwetsbaarheden;

4) erop toezien dat een methode ten uitvoer wordt gelegd om de informatie indien nodig intern te verspreiden.

c) Elke gecontracteerde organisatie die de organisatie kan blootstellen aan informatiebeveiligingsrisico's met potentiële gevolgen voor de veiligheid van de luchtvaart moet informatiebeveiligingsvoorvallen melden aan de organisatie. Deze meldingen worden ingediend volgens de procedures die in de specifieke contractuele regelingen zijn vastgesteld en worden geëvalueerd overeenkomstig punt b).

d) De organisatie pleegt overleg over onderzoeken met elke andere organisatie die een belangrijke bijdrage levert aan de informatiebeveiliging van haar eigen activiteiten.

e) De organisatie mag dat rapportagesysteem integreren in andere rapportagesystemen die zij reeds toepast.

IS.D.OR.220 Informatiebeveiligingsincidenten — opsporing, reactie en herstel

a) Op basis van de resultaten van de overeenkomstig IS.D.OR.205 en IS.D.OR.210 uitgevoerde risicobehandelingen, past de organisatie maatregelen toe om incidenten en kwetsbaarheden op te sporen die erop wijzen dat zich onaanvaardbare risico's kunnen voordoen die potentiële gevolgen kunnen hebben voor de veiligheid van de luchtvaart. Die opsporingsmaatregelen moeten de organisatie in staat stellen om:

1) afwijking van vooraf bepaalde referentiescenario's voor functionele prestaties vast te stellen;

2) waarschuwingen te geven om passende responsmaatregelen te activeren in geval van een afwijking.

b) De organisatie past maatregelen toe om te reageren op overeenkomstig punt a) vastgestelde voorvalsomstandigheden die zich kunnen ontwikkelen of hebben ontwikkeld tot een informatiebeveiligingsincident. Die responsmaatregelen moeten de organisatie in staat stellen om:

1) te reageren op de in punt a), 2), bedoelde waarschuwingen door vooraf gedefinieerde middelen en acties te activeren;

2) de verspreiding van een aanval in te dammen en te voorkomen dat het dreigingsscenario volledig werkelijkheid wordt;

3) de faalwijze van de in IS.D.OR.205, punt a), gedefinieerde getroffen elementen te controleren.

c) De organisatie voert maatregelen uit die gericht zijn op herstel van informatiebeveiligingsincidenten, met inbegrip van noodmaatregelen, indien nodig. Die herstelmaatregelen moeten de organisatie in staat stellen om:

1) de omstandigheid die het incident heeft veroorzaakt, weg te nemen of tot een aanvaardbaar niveau te beperken;

2) een veilige toestand te bereiken van de in IS.D.OR.205, punt a), gedefinieerde getroffen elementen, binnen een vooraf door de organisatie vastgestelde hersteltijd.

IS.D.OR.225 Reactie op door de bevoegde autoriteit gemelde bevindingen

a) Na ontvangst van de door de bevoegde autoriteit ingediende kennisgeving van bevindingen, moet de organisatie:

1) de fundamentele oorzaak of oorzaken van het geval van niet-naleving identificeren, alsook de factoren die ertoe hebben bijgedragen;

2) een corrigerend actieplan opstellen;

3) tot voldoening van de bevoegde autoriteit aantonen dat de niet-naleving is gecorrigeerd.

b) De in punt a) vermelde acties worden uitgevoerd binnen de met de bevoegde autoriteit overeengekomen termijn.

IS.D.OR.230 Regeling voor externe rapportage over informatiebeveiliging

a) De organisatie past een systeem voor informatiebeveiligingsmeldingen toe dat overeenstemt met de in Verordening (EU) nr. 376/2014 en de gedelegeerde en uitvoeringshandelingen daarvan vastgestelde eisen, als die verordening op de organisatie van toepassing is.

b) Onverminderd de verplichtingen van Verordening (EU) nr. 376/2014 ziet de organisatie erop toe dat alle incidenten of kwetsbaarheden op het gebied van informatiebeveiliging die een aanzienlijk risico voor de veiligheid van de luchtvaart kunnen vormen, aan hun bevoegde autoriteit worden gemeld. Bovendien

1) als een incident of kwetsbaarheid gevolgen heeft voor een luchtvaartuig of bijbehorende systemen of componenten, moet de organisatie dit ook melden aan de houder van de ontwerpgoedkeuring;

2) als een incident of kwetsbaarheid gevolgen heeft voor door de organisatie gebruikte systemen of onderdelen, moet de organisatie dit melden aan de organisatie die verantwoordelijk is voor het ontwerp van het systeem of onderdeel.

c) De organisatie rapporteert de in punt b) bedoelde voorwaarden als volgt:

1) zodra de organisatie weet krijgt van de omstandigheid, wordt een kennisgeving ingediend bij de bevoegde autoriteit en, indien van toepassing, de houder van de ontwerpgoedkeuring of de organisatie die verantwoordelijk is voor het ontwerp van het systeem of onderdeel;

2) zo snel mogelijk, maar uiterlijk 72 uur na het tijdstip waarop de organisatie weet heeft gekregen van de omstandigheid, tenzij uitzonderlijke omstandigheden dit verhinderen, wordt een verslag ingediend bij de bevoegde autoriteit en, indien van toepassing, de houder van de ontwerpgoedkeuring of de organisatie die verantwoordelijk is voor het ontwerp van het systeem of onderdeel.

Het verslag wordt opgesteld in de door de bevoegde autoriteit bepaalde vorm en bevat alle relevante informatie over de omstandigheid waar de organisatie weet van heeft;

3) er wordt een follow-upverslag ingediend bij de bevoegde autoriteit en, indien van toepassing, de houder van de ontwerpgoedkeuring of de organisatie die verantwoordelijk is voor het ontwerp van het systeem of onderdeel, met nadere informatie over de acties die de organisatie heeft genomen of voornemens is te nemen om van het incident te herstellen en de acties die zij voornemens is te nemen om soortgelijke informatiebeveiligingsincidenten in de toekomst te voorkomen.

Het follow-upverslag wordt ingediend zodra deze maatregelen zijn vastgesteld, en wordt opgesteld in de door de bevoegde autoriteit vastgestelde vorm.

IS.D.OR.235 Uitbesteding van activiteiten op het gebied van informatiebeveiligingsbeheer

a) De organisatie ziet erop toe dat bij het uitbesteden van een deel van de in IS.D.OR.200 bedoelde activiteiten aan andere organisaties, de uitbestede activiteiten voldoen aan de eisen van deze verordening en dat de gecontracteerde organisatie onder haar toezicht werkt. De organisatie zorgt ervoor dat de risico's in verband met de uitbestede activiteiten op passende wijze worden beheerd.

b) De organisatie ziet erop toe dat de bevoegde autoriteit op verzoek toegang krijgt tot de gecontracteerde organisatie om na te gaan of zij blijvend de in deze verordening vastgestelde toepasselijke eisen naleeft.

IS.D.OR.240 Eisen met betrekking tot personeel

a) De verantwoordelijke manager van de organisatie of, in het geval van ontwerporganisaties, het hoofd van de ontwerporganisatie, aangewezen overeenkomstig Verordening (EU) nr. 748/2012 en Verordening (EU) nr. 139/2014 als bedoeld in artikel 2, punt 1), a) en b), van deze verordening, hebben binnen de organisatie de bevoegdheid om ervoor te zorgen dat alle krachtens deze verordening vereisten activiteiten kunnen worden gefinancierd en uitgevoerd. Die persoon moet:

1) ervoor zorgen dat alle nodige middelen beschikbaar zijn om aan de voorschriften van deze verordening te voldoen;

2) het in IS.D.OR.200, punt a), 1), bedoelde informatiebeveiligingsbeleid vaststellen en bevorderen;

3) blijk geven van een fundamenteel begrip van deze verordening.

b) De verantwoordelijke manager of, in het geval van ontwerporganisaties, het hoofd van de ontwerporganisatie benoemt een persoon of een groep personen die ervoor moet zorgen dat de organisatie in overeenstemming is met de eisen van deze verordening, en stelt de reikwijdte van hun bevoegdheden vast. Die persoon of groep personen brengt rechtstreeks verslag uit aan de verantwoordelijke manager of, in het geval van ontwerporganisaties, aan het hoofd van de ontwerporganisatie, en beschikt over de nodige kennis, achtergrond en ervaring om zich van zijn verantwoordelijkheden te kwijten. Voorts wordt ook vastgesteld wie bij langdurige afwezigheid van een bepaalde persoon als plaatsvervanger optreedt.

c) De verantwoordelijke manager of, in het geval van ontwerporganisaties, het hoofd van de ontwerporganisatie benoemt een persoon of een groep personen die verantwoordelijk is voor het beheer van de in IS.D.OR.200, punt a), 12), bedoelde functie voor toezicht op de naleving.

d) Als de organisatie organisatorische structuren, beleid, processen en procedures voor informatiebeveiliging deelt met andere organisaties of met afdelingen van de eigen organisatie die niet onder de goedkeuring of verklaring vallen, mag de verantwoordelijke manager of, in het geval van ontwerporganisaties, het hoofd van de ontwerporganisatie zijn activiteiten delegeren aan een gemeenschappelijke verantwoordelijke persoon.

In dat geval worden coördinatiemaatregelen vastgesteld tussen de verantwoordelijke manager van de organisatie of, in het geval van ontwerporganisaties, het hoofd van de ontwerporganisatie, en de gemeenschappelijke verantwoordelijke persoon om de passende integratie van het informatiebeveiligingsbeheer in de organisatie te waarborgen.

e) De verantwoordelijke manager of het hoofd van de ontwerporganisatie, of de in punt d) bedoelde gemeenschappelijke verantwoordelijke persoon, is binnen de organisatie bevoegd voor de vaststelling en instandhouding van de organisatorische structuren, het beleid en de processen en procedures die nodig zijn voor de uitvoering van IS.D.OR.200.

f) De organisatie beschikt over een proces om ervoor te zorgen dat zij over voldoende personeel beschikt om de onder deze bijlage vallende activiteiten uit te voeren.

g) De organisatie beschikt over een proces om ervoor te zorgen dat het in punt f) bedoelde personeel over de nodige bekwaamheid beschikt om zijn taken uit te voeren.

h) De organisatie beschikt over een proces om ervoor te zorgen dat het personeel de aan de toegewezen rollen en taken verbonden verantwoordelijkheden erkent.

i) De organisatie zorgt ervoor dat de identiteit en betrouwbaarheid van het personeel dat toegang heeft tot informatiesystemen en gegevens waarop de eisen van deze verordening van toepassing zijn, op passende wijze worden vastgesteld.

IS.D.OR.245 Bijhouden van gegevens

a) De organisatie houdt gegevens bij over haar activiteiten op het gebied van informatiebeveiligingsbeheer.

1) De organisatie zorgt ervoor dat de volgende gegevens worden gearchiveerd en traceerbaar zijn:

i) alle ontvangen goedkeuringen en eventuele bijbehorende beoordelingen van de informatiebeveiligingsrisico's overeenkomstig IS.D.OR.200, punt e);

ii) contracten voor de in IS.D.OR.200, punt a), 9), bedoelde activiteiten;

iii) gegevens over de in IS.D.OR.200, punt d), bedoelde cruciale processen;

iv) gegevens over de risico's die zijn vastgesteld tijdens de in IS.D.OR.205 bedoelde risicobeoordeling, samen met de in IS.D.OR.210 bedoelde maatregelen voor het aanpakken van die risico's;

v) gegevens over informatiebeveiligingsincidenten en kwetsbaarheden die gerapporteerd zijn overeenkomstig de in IS.D.OR.215 en IS.D.OR.230 bedoelde rapportageregelingen;

vi) gegevens over informatiebeveiligingsvoorvallen die mogelijk opnieuw moeten worden beoordeeld om onopgespoorde informatiebeveiligingsincidenten of kwetsbaarheden te ontdekken.

2) De in punt 1), i), bedoelde gegevens worden bewaard gedurende minstens vijf jaar nadat de geldigheid van de goedkeuring is verstreken.

3) De in punt 1), ii), bedoelde gegevens worden bewaard gedurende minstens vijf jaar nadat het contract is gewijzigd of beëindigd.

4) De in punt 1), iii), iv) en v), bedoelde gegevens worden minstens vijf jaar bewaard.

5) De in punt 1), vi), bedoelde gegevens worden bewaard totdat die informatiebeveiligingsvoorvallen opnieuw zijn beoordeeld overeenkomstig een frequentie die is vastgesteld in een door de organisatie opgestelde procedure.

b) De organisatie houdt gegevens bij over de kwalificaties en ervaring van haar eigen personeel dat betrokken is bij activiteiten op het gebied van informatiebeveiligingsbeheer.

1) De gegevens over de kwalificaties en ervaring van het personeel moeten worden bewaard zolang de persoon in kwestie voor de organisatie werkt, en gedurende minstens drie jaar nadat hij de organisatie heeft verlaten.

2) Indien personeelsleden daarom verzoeken, moeten zij toegang krijgen tot hun persoonlijke gegevens. Wanneer zij de organisatie verlaten, moet de organisatie hen, op verzoek, een kopie geven van hun individuele gegevens.

c) De vorm van de gegevens wordt gespecificeerd in de procedures van de organisatie.

d) De gegevens worden zodanig opgeslagen dat zij beschermd zijn tegen schade, wijziging en diefstal, waarbij in voorkomend geval informatie wordt geïdentificeerd volgens het rubriceringsniveau. De organisatie zorgt ervoor dat de gegevens worden opgeslagen met behulp van middelen die de integriteit, authenticiteit en geautoriseerde toegang waarborgen.

IS.D.OR.250 Handboek informatiebeveiligingsbeheer

a) De organisatie verstrekt de bevoegde autoriteit een handboek informatiebeveiligingsbeheer en, indien van toepassing, alle bijbehorende handleidingen en procedures, die het volgende bevatten:

1) een verklaring die is ondertekend door de verantwoordelijke manager of, in het geval van ontwerporganisaties, het hoofd van de ontwerporganisatie, waarin wordt bevestigd dat de organisatie te allen tijde zal handelen overeenkomstig deze bijlage en het handboek informatiebeveiligingsbeheer. Als de verantwoordelijke manager of, in het hoofd van de ontwerporganisatie, het hoofd van de ontwerporganisatie, niet de algemeen directeur (CEO) van de organisatie is, dan moet die CEO de verklaring medeondertekenen;

2) de titel(s), na(a)m(en), verantwoordelijkheden en bevoegdheden van de in IS.D.OR.240, punten b) en c), bedoelde persoon of personen;

3) de titel, naam, taken, verantwoordelijkheden en bevoegdheden van de in IS.D.OR.240, punt d), bedoelde gemeenschappelijke verantwoordelijke persoon, indien van toepassing;

4) het informatiebeveiligingsbeleid van de organisatie, zoals bedoeld in IS.D.OR.200, punt a), 1);

5) een algemene beschrijving van het aantal en de categorieën personeelsleden en van het systeem om de beschikbaarheid van personeel te plannen, zoals vereist bij IS.D.OR.240;

6) de titel(s), na(a)m(en), verantwoordelijkheden en bevoegdheden van de belangrijkste personen die verantwoordelijk zijn voor de uitvoering van IS.D.OR.200, met inbegrip van de persoon of personen die verantwoordelijk is (zijn) voor de in IS.D.OR.200, punt a), 12), bedoelde functie toezicht op de naleving;

7) een organisatieschema met de bijbehorende aansprakelijkheids- en verantwoordelijkheidsketens voor de in de punten 2) en 6) bedoelde personen;

8) de beschrijving van het in IS.D.OR.215 bedoelde interne rapportagesysteem;

9) de procedures waarin gespecificeerd is hoe de organisatie de naleving van dit deel waarborgt, en met name:

i) de documentatie in IS.D.OR.200, punt c);

ii) de procedures die bepalen hoe de organisatie de in IS.D.OR.200, punt a), 9), bedoelde gecontracteerde activiteiten controleert;

iii) de procedure voor de wijziging van het in punt c) bedoelde handboek informatiebeveiligingsbeheer;

10) de bijzonderheden van de op dit moment goedgekeurde alternatieve wijzen van naleving.

b) De eerste uitgave van het handboek informatiebeveiligingsbeheer wordt goedgekeurd en een kopie ervan wordt bewaard door de bevoegde autoriteit. Het handboek informatiebeveiligingsbeheer dient zo nodig te worden gewijzigd om een actuele beschrijving van het beheersysteem voor informatiebeveiliging van de organisatie te blijven bieden. Een kopie van eventuele wijzigingen van het handboek informatiebeveiligingsbeheer wordt verstrekt aan de bevoegde autoriteit.

c) Wijzigingen van het handboek informatiebeveiligingsbeheer worden beheer volgens een door de organisatie vastgestelde procedure. Alle wijzigingen die buiten het toepassingsgebied van deze procedure vallen en alle amendementen van de in IS.D.OR.255, punt b), bedoelde wijzigingen moeten worden goedgekeurd door de bevoegde autoriteit.

d) De organisatie mag het handboek informatiebeveiligingsbeheer integreren met andere managementhandboeken of handleidingen, voor zover er een duidelijke kruisverwijzing is die aangeeft welke delen van het managementhandboek of de handleiding overeenstemmen met de verschillende eisen van deze bijlage.

IS.D.OR.255 Wijzigingen van het beheersysteem voor informatiebeveiliging

a) Wijzigingen van het beheersysteem voor informatiebeveiliging worden beheerd en meegedeeld aan de bevoegde autoriteit volgens een door de organisatie ontwikkelde procedure. Deze procedure moet worden goedgekeurd door de bevoegde autoriteit.

b) Voor wijzigingen van het beheersysteem voor informatiebeveiliging die niet onder de in punt a) bedoelde procedure vallen, moet de organisatie bij de bevoegde autoriteit een goedkeuring aanvragen en verkrijgen.

Wat deze wijzigingen betreft:

1) wordt de aanvraag ingediend alvorens een dergelijke wijziging wordt doorgevoerd, zodat de bevoegde autoriteit kan bepalen of er nog altijd wordt voldaan aan deze verordening en zo nodig het certificaat van de organisatie en de bijbehorende voorwaarden van de goedkeuring kan aanpassen;

2) verstrekt de organisatie aan de bevoegde autoriteit alle informatie die zijn vraag om de wijziging te evalueren;

3) de wijziging wordt pas doorgevoerd na ontvangst van een formele goedkeuring door de bevoegde autoriteit;

4) tijdens de uitvoering van dergelijke wijzigingen werkt de organisatie onder de door de bevoegde autoriteit voorgeschreven voorwaarden.

IS.D.OR.260 Permanente verbetering

a) De organisatie beoordeelt aan de hand van passende prestatie-indicatoren de doeltreffendheid en maturiteit van het beheersysteem voor informatiebeveiliging. Die beoordeling wordt uitgevoerd op basis van een vooraf door de organisatie vastgestelde kalender of na een informatiebeveiligingsincident.

b) Als na de overeenkomstig punt a) uitgevoerde beoordeling tekortkomingen worden vastgesteld, neemt de organisatie de nodige verbeteringsmaatregelen om te garanderen dat het beheersysteem voor informatiebeveiliging blijft voldoen aan de toepasselijke eisen en de informatiebeveiligingsrisico's op een aanvaardbaar niveau handhaaft. De organisatie zal de elementen van het beheersysteem voor informatiebeveiliging die onder de vastgestelde maatregelen vallen, opnieuw beoordelen.