Raad van de
Europese Unie

Brussel, 18 juli 2022
(OR. en)

11468/22
ADD 1

AVIATION 171
DELACT 120

BEGELEIDENDE NOTA

van:	de secretaris-generaal van de Europese Commissie, ondertekend door mevrouw Martine DEPREZ, directeur
ingekomen:	14 juli 2022
aan:	het secretariaat-generaal van de Raad
nr. Comdoc.:	C(2022) 4882 final - ANNEX
Betreft:	BIJLAGE bij de GEDELEGEERDE VERORDENING VAN DE COMMISSIE 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 nr. 139/2014 van de Commissie vallen en tot wijziging van Verordeningen (EU) nr. 748/2012 en nr. 139/2014 van de Commissie

Hierbij gaat voor de delegaties document C(2022) 4882 final - ANNEX.

Bijlage: C(2022) 4882 final - ANNEX

EUROPESE
COMMISSIE

Brussel, 14.7.2022
C(2022) 4882 final

ANNEX

BIJLAGE

bij

GEDELEGEERDE VERORDENING VAN DE COMMISSIE

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 nr. 139/2014 van de Commissie vallen en tot wijziging van Verordeningen (EU) nr. 748/2012 en nr. 139/2014 van de Commissie

BIJLAGE

INFORMATIEBEVEILIGING — VEREISTEN VAN DE ORGANISATIE

[PART-IS.D.OR]

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, 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, 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, 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([1]) en de eisen van IS.D.OR.200, 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;

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

([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).

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, 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, 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, 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, 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 onder 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, 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, 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, e);

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

iii) gegevens over de in IS.D.OR.200, 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 5 jaar nadat de geldigheid van de goedkeuring is verstreken.

3) De in punt 1), ii), bedoelde gegevens worden bewaard gedurende minstens 5 jaar nadat het contract is gewijzigd of beëindigd.

4) De in punt 1), iii), iv) en v), bedoelde gegevens worden minstens 5 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 3 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 tijd 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, b) en c), bedoelde persoon of personen;

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

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

ii) de procedures die bepalen hoe de organisatie de in IS.D.OR.200, 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, 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.