BESLUIT (EU, Euratom) 2018/559 VAN DE COMMISSIE

van 6 april 2018

tot vaststelling van uitvoeringsbepalingen voor artikel 6 van Besluit (EU, Euratom) 2017/46 over de beveiliging van communicatie- en informatiesystemen binnen de Europese Commissie

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 249,

Gezien het Verdrag tot oprichting van de Europese Gemeenschap voor Atoomenergie,

Gezien Besluit (EU, Euratom) 2017/46 van de Commissie van 10 januari 2017 over de beveiliging van communicatie- en informatiesystemen binnen de Europese Commissie ([1]), en met name artikel 6,

Overwegende hetgeen volgt:

(1) Door de goedkeuring van Besluit (EU, Euratom) 2017/46 moet de Commissie de uitvoeringsbepalingen in verband met het ingetrokken Besluit C(2006) 3602 van de Commissie over de beveiliging van communicatie- en informatiesystemen binnen de Europese Commissie herzien, bijwerken en consolideren.

(2) De commissaris die bevoegd is voor beveiliging heeft, overeenkomstig het reglement van orde, de bevoegdheid gekregen uitvoeringsbepalingen vast te stellen overeenkomstig artikel 13 van Besluit (EU, Euratom) 2017/46 ([2]).

(3) De uitvoeringsbepalingen van Besluit C(2006) 3602 moeten bijgevolg worden ingetrokken,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

HOOFDSTUK 1

ALGEMENE BEPALINGEN

Artikel 1

Onderwerp en toepassingsgebied

1. Het onderwerp en toepassingsgebied van dit besluit zijn bepaald in artikel 1 van Besluit (EU, Euratom) 2017/46.

2. Dit besluit is van toepassing op alle communicatie- en informatiesystemen (hierna „CIS" genoemd). De in dit besluit bepaalde verantwoordelijkheden zijn echter niet van toepassing op CIS'en waarin gerubriceerde informatie van de EU wordt verwerkt. De verantwoordelijkheden voor die systemen zullen worden vastgesteld door de systeemeigenaar en de Veiligheidsautoriteit van de Commissie, overeenkomstig Besluit (EU, Euratom) 2015/444 van de Commissie ([3]).

3. Hoofdstuk 2 van het onderhavige besluit bevat een overzicht van de praktische uitvoering van de organisatie en de verantwoordelijkheden met betrekking tot IT-beveiliging. Hoofdstuk 3 van het onderhavige besluit bevat een overzicht van de processen die verband houden met artikel 6 van Besluit (EU, Euratom) 2017/46.

Artikel 2

Definities

De definities van artikel 2 van Besluit (EU, Euratom) 2017/46 gelden voor dit besluit. Voorts gelden voor de toepassing van dit besluit ook de volgende definities:

1. „Crypto Approval Authority" (autoriteit voor de goedkeuring van encryptieproducten, CAA) is een functie die wordt bekleed door de Veiligheidsautoriteit van de Commissie, die ressorteert onder de directeur-generaal Personele Middelen en Veiligheid;

([1]) PB L 6 van 11.1.2017, blz. 40.
([2]) Besluit C(2017) 7428 final van de Commissie van 8 november 2017 waarbij een machtiging wordt verleend voor de goedkeuring van uitvoeringsbepalingen, normen en richtlijnen met betrekking tot de beveiliging van communicatie- en informatiesystemen in de Europese Commissie.
([3]) Besluit (EU, Euratom) 2015/444 van de Commissie van 13 maart 2015 betreffende de veiligheidsvoorschriften voor de bescherming van gerubriceerde EU-informatie (PB L 72 van 17.3.2015, blz. 53).

2. „externe netwerkverbinding" is een elektronische communicatieverbinding tussen het interne netwerk van de Commissie en een ander netwerk, met inbegrip van het internet. Netwerken van derde partijen die in het kader van een contract deel uitmaken van het interne netwerk van de Commissie, vallen niet onder deze definitie;

3. „key-escrow" is een procedure voor het opslaan van kopieën van cryptografische sleutels bij een of meer aparte partijen, waarbij de scheiding van functies wordt gewaarborgd, zodat zij kunnen worden hersteld als de operationele kopie verloren gaat. Sleutels kunnen in twee of meer delen worden opgesplitst en elk deel wordt door een andere partij bewaard zodat geen enkele partij de volledige sleutel in haar bezit heeft;

4. „RASCI" is de afkorting voor een verdeling van verantwoordelijkheden op basis van de volgende kenmerken:

   a) „verantwoordelijk" (*responsible*, R): de verplichting hebbend om op te treden en besluiten te nemen om de vereiste resultaten tot stand te brengen;

   b) „verantwoordingsplichtig" (*accountable*, A): de verplichting hebbend om verantwoording af te leggen met betrekking tot acties, besluiten en prestaties;

   c) „ondersteunend" (*supporting*, S): de verplichting hebbend om met de verantwoordelijke samen te werken om de taak te voltooien;

   d) „geraadpleegd" (*consulted*, C): gevraagd om advies of mening;

   e) „geïnformeerd" (*informed*, I): beschikkend over recente en nuttige informatie.

HOOFDSTUK 2

ORGANISATIE EN VERANTWOORDELIJKHEDEN

Artikel 3

Taken en verantwoordelijkheden

De taken en verantwoordelijkheden met betrekking tot de artikelen 4 tot en met 8 van dit besluit worden gedefinieerd in de bijlage overeenkomstig het RASCI-model.

Artikel 4

Aanpassing aan het informatiebeveiligingsbeleid van de Commissie

1. Het directoraat-generaal Personele Middelen en Veiligheid zal het IT-beveiligingsbeleid van de Commissie en de bijhorende normen en richtlijnen evalueren om na te gaan of zij stroken met het algemene veiligheidsbeleid van de Commissie, en specifiek met Besluit (EU, Euratom) 2015/443 van de Commissie ([1]) en Besluit (EU, Euratom) 2015/444.

2. Op verzoek van andere afdelingen van de Commissie kan het directoraat-generaal Personele Middelen en Veiligheid nagaan of hun beleid inzake IT-beveiliging of andere IT-beveiligingsdocumentatie strookt met het informatiebeveiligingsbeleid van de Commissie. Het eenheidshoofd van die afdeling zorgt er dan voor dat eventuele inconsistenties worden aangepakt.

3. Het directoraat-generaal Personele Middelen en Veiligheid zorgt er als verantwoordelijke voor informatiebeveiliging samen met het directoraat-generaal Informatica voor dat in de IT-beveiligingsprocessen ten volle rekening wordt gehouden met de rubricering en beginselen inzake veiligheid zoals bepaald in Besluit (EU, Euratom) 2015/443, en met name de artikelen 3 en 9.

HOOFDSTUK 3

IT-BEVEILIGINGSPROCESSEN

Artikel 5

Encryptietechnologie

1. Bij het gebruik van encryptietechnologie voor de bescherming van gerubriceerde EU-informatie moet worden voldaan aan Besluit (EU, Euratom) 2015/444.

2. De besluiten over het gebruik van encryptietechnologie voor de bescherming van niet-gerubriceerde EU-informatie worden genomen door de systeemeigenaar van ieder CIS, daarbij rekening houdend met zowel de risico's die door de encryptie moeten worden voorkomen als de risico's die door de encryptie ontstaan.

3. Voorafgaande goedkeuring door de CAA is vereist voor elk gebruik van encryptietechnologie, tenzij de encryptie alleen wordt gebruikt ter bescherming van de vertrouwelijkheid van niet-gerubriceerde EU-informatie bij het doorsturen en er gebruikgemaakt wordt van standaardnetwerkcommunicatieprotocollen.

([1]) Besluit (EU, Euratom) 2015/443 van de Commissie van 13 maart 2015 betreffende veiligheid binnen de Commissie (PB L 72 van 17.3.2015, blz. 41).

4. Met uitzondering van lid 3 van dit artikel zorgen de afdelingen van de Commissie voor back-ups van decryptiesleutels die in „key-escrow" zijn opgeslagen, zodat de opgeslagen gegevens kunnen worden gerecupereerd als de decryptiesleutel niet beschikbaar is. Versleutelde gegevens mogen slechts uit een back-up worden gerecupereerd als daartoe toestemming is verleend overeenkomstig de door de CAA vastgestelde norm.

5. Verzoeken om toestemming voor het gebruik van encryptietechnologie moeten formeel gedocumenteerd zijn en details bevatten over het CIS en de te beschermen gegevens, de te gebruiken technologie en de bijhorende operationele beveiligingsprocedures. Deze verzoeken om toestemming moeten worden ondertekend door de systeemeigenaar.

6. De CAA evalueert een verzoek om toestemming voor het gebruik van encryptietechnologie overeenkomstig de gepubliceerde normen en vereisten.

Artikel 6

IT-veiligheidsinspecties

1. Het directoraat-generaal Personele Middelen en Veiligheid voert IT-beveiligingsinspecties uit om na te gaan of de IT-veiligheidsmaatregelen stroken met het beleid van de Commissie inzake IT-beveiliging en om de integriteit van deze controlemaatregelen te onderzoeken.

2. Het directoraat-generaal Personele Middelen en Veiligheid kan een IT-beveiligingsinspectie uitvoeren:

a) op eigen initiatief;

b) op verzoek van de stuurgroep voor informatiebeveiliging (ISSB);

c) op verzoek van een systeemeigenaar;

d) na een veiligheidsincident, of

e) na de ontdekking van een hoog risico in een bepaald systeem.

3. Gegevenseigenaars kunnen een IT-beveiligingsinspectie vragen voordat zij hun informatie opslaan in een CIS.

4. De resultaten van een inspectie worden gedocumenteerd in een formeel verslag aan de systeemeigenaar, met een kopie aan de LISO, waarin bevindingen en aanbevelingen staan over hoe het CIS beter kan worden afgestemd op het IT-beveiligingsbeleid. Het directoraat-generaal Personele Middelen en Veiligheid brengt verslag uit over belangrijke kwesties en aanbevelingen aan de ISSB.

5. Het directoraat-generaal Personele Middelen en Veiligheid ziet toe op de uitvoering van de aanbevelingen.

6. Waar nodig houden IT-beveiligingsinspecties de inspectie in van diensten, locaties en apparatuur die ter beschikking staan van de systeemeigenaar, met inbegrip van interne en externe dienstverleners.

Artikel 7

Toegang via externe netwerken

1. Het directoraat-generaal Personele Middelen en Veiligheid bepaalt de regels in een norm over het toestaan van toegang tussen CIS'en van de Commissie en externe netwerken.

2. In de regels wordt een onderscheid gemaakt tussen de verschillende types externe netwerkverbindingen en worden voor elk type verbinding passende veiligheidsregels bepaald, onder meer of voor de verbinding voorafgaande toestemming van de bevoegde autoriteit als bedoeld in lid 4 is vereist.

3. Indien vereist, wordt de toestemming verleend op basis van een formele procedure voor aanvraag en goedkeuring. De goedkeuring geldt voor een bepaalde periode en moet worden verkregen voordat de verbinding wordt geactiveerd.

4. Het directoraat-generaal Personele Middelen en Veiligheid is verantwoordelijk voor de verzoeken om toestemming, maar kan de verantwoordelijkheid voor een aantal types verbindingen naar eigen goeddunken delegeren overeenkomstig Besluit (EU, Euratom) 2015/443, artikel 17, lid 3, en onder de in lid 8 bepaalde voorwaarden.

5. De toestemmingverlenende entiteit kan aanvullende beveiligingsvereisten opleggen als voorwaarde voor de toestemming, om zo de CIS'en en netwerken van de Commissie te beschermen tegen ongeoorloofde toegang of andere veiligheidslekken.

6. Het directoraat-generaal Informatica is de standaardverlener van netwerkdiensten voor de Commissie. Elke afdeling van de Commissie die een netwerk gebruikt dat niet is geleverd door het directoraat-generaal Informatica, verzoekt eerst de ISSB om toestemming. De afdeling van de Commissie moet het verzoek op operationele gronden motiveren en aantonen dat de netwerkcontroles volstaan om te voldoen aan de vereisten inzake controle van in- en uitgaande informatiestromen.

7. De systeemeigenaar van een CIS bepaalt de beveiligingsvereisten voor externe toegang tot dat CIS en zorgt voor de uitvoering van gepaste maatregelen om de beveiliging ervan te beschermen, met ondersteuning van de LISO.

8. De veiligheidsmaatregelen voor externe netwerkverbindingen zijn gebaseerd op de beginselen van *need-to-know* (noodzaak tot kennisneming) en *least privilege* (alleen strikt noodzakelijke rechten worden toegekend).

9. Alle externe netwerkverbindingen worden gefilterd en gemonitord om mogelijke veiligheidslekken op te sporen.

10. Als verbindingen tot stand worden gebracht om een CIS te kunnen uitbesteden, geldt voor de toestemming de voorwaarde dat de in artikel 8 beschreven procedure moet zijn voltooid.

Artikel 8

Uitbesteden van CIS'en

1. Voor de toepassing van dit besluit wordt een CIS beschouwd als uitbesteed als het wordt verstrekt op basis van een contract met een derde partij, waarbij het CIS zich niet in een gebouw van de Commissie bevindt. Dit omvat ook het uitbesteden van individuele of meerdere CIS'en of andere IT-diensten, datacentra in gebouwen die niet van de Commissie zijn en het behandelen van datasets van de Commissie door externe diensten.

2. Bij het uitbesteden van een CIS wordt op de volgende manier rekening gehouden met de gevoeligheid of rubricering van de behandelde informatie:

a) een CIS dat gerubriceerde EU-informatie bevat, wordt gehomologeerd overeenkomstig Besluit (EU, Euratom) 2015/444, en de Veiligheidshomologatieautoriteit (SAA) wordt vooraf geraadpleegd. Systemen die gerubriceerde EU-informatie bevatten, mogen niet worden uitbesteed;

b) de systeemeigenaar van een CIS dat niet-gerubriceerde EU-informatie bevat, neemt evenredige beveiligingsmaatregelen die overeenstemmen met de geldende wettelijke verplichtingen of de gevoeligheid van de informatie, rekening houdend met de risico's van uitbesteding. Het directoraat-generaal Personele Middelen en Veiligheid kan aanvullende vereisten opleggen;

c) bij uitbestede ontwikkelingsprojecten moet rekening worden gehouden met de gevoeligheid van de ontwikkelde code en van testgegevens die tijdens de ontwikkeling worden gebruikt.

3. De volgende beginselen zijn van toepassing op uitbestede CIS'en, bovenop de in Besluit (EU, Euratom) 2017/46, artikel 3, bepaalde beginselen:

a) bij uitbestedingsregelingen moet afhankelijkheid van specifieke leveranciers worden voorkomen;

b) bij regelingen inzake de beveiliging van uitbesteding moeten de mogelijkheden voor personeel van een derde om toegang te krijgen tot Commissie-informatie of deze te wijzigen, zo veel mogelijk worden beperkt;

c) personeel van een derde dat toegang heeft tot uitbestede CIS'en, moet een geheimhoudingsovereenkomst voorleggen;

d) in de inventaris van CIS'en wordt aangegeven of een CIS is uitbesteed.

4. De systeemeigenaar moet, samen met de gegevenseigenaar:

a) de risico's van uitbesteding beoordelen en documenteren;

b) beveiligingsvereisten vastleggen;

c) de systeemeigenaars van alle ermee verbonden CIS'en raadplegen om ervoor te zorgen dat aan hun beveiligingsvereisten wordt voldaan;

d) gepaste beveiligingsvereisten en rechten opnemen in het uitbestedingscontract;

e) voldoen aan de andere vereisten van de in lid 8 genoemde gedetailleerde procedure.

Deze acties moeten voltooid zijn voordat het contract of een andere overeenkomst voor het uitbesteden van één of meer CIS'en wordt ondertekend.

5. Systeemeigenaars beheren de risico's van uitbesteding tijdens de levensduur van het CIS om te voldoen aan de vastgestelde beveiligingsvereisten.

6. Systeemeigenaars zien erop toe dat externe contractanten verplicht zijn de Commissie meteen in te lichten over elk IT-beveiligingsincident dat een uitbesteed CIS van de Commissie treft.

7. De systeemeigenaar zorgt voor de conformiteit van het CIS, het aanbestedingscontract en de beveiligingsregelingen met de regels van de Commissie over informatiebeveiliging en IT-beveiliging.

8. Het directoraat-generaal Personele Middelen en Veiligheid bepaalt de gedetailleerde normen voor de onder 1 tot en met 7 bepaalde verantwoordelijkheden en activiteiten overeenkomstig artikel 10.

HOOFDSTUK 4

DIVERSE EN SLOTBEPALINGEN

Artikel 9

Transparantie

Dit besluit wordt onder de aandacht gebracht van alle personeelsleden van de Commissie en alle personen op wie het van toepassing is, en wordt bekendgemaakt in het *Publicatieblad van de Europese Unie*.

Artikel 10

Normen

1. De bepalingen van dit besluit worden, waar nodig, nader gedetailleerd in normen en/of richtsnoeren die moeten worden goedgekeurd overeenkomstig Besluit (EU, Euratom) 2017/46 en Besluit C(2017) 7428. IT-beveiligingsnormen en richtlijnen geven meer details over deze uitvoeringsbepalingen en Besluit (EU, Euratom) 2017/46 inzake specifieke beveiligingsdomeinen volgens ISO 27001:2013 bijlage A. Deze normen en richtlijnen zijn gebaseerd op beste prakijken in de sector en worden gekozen op maat van de IT-omgeving van de Commissie.

2. Normen worden, waar nodig, ontwikkeld overeenkomstig ISO 27001:2013 bijlage A op de volgende domeinen:

(1) organisatie van informatiebeveiliging;

(2) beveiliging van personeel;

(3) beheer van activa;

(4) toegangscontrole;

(5) cryptografie;

(6) fysieke en omgevingsbeveiliging;

(7) operationele veiligheid;

(8) communicatiebeveiliging;

(9) aankoop, ontwikkeling en onderhoud van systemen;

(10) leveranciersrelaties;

(11) beheer van incidenten op het gebied van informatiebeveiliging;

(12) informatiebeveiligingsaspecten van beheer van de bedrijfscontinuïteit;

(13) naleving.

3. Alvorens de in de leden 1 en 2 bedoelde normen worden vastgesteld, worden zij ter goedkeuring voorgelegd aan de ISSB.

4. De uitvoeringsbepalingen van Besluit C(2006) 3602 betreffende het toepassingsgebied van dit besluit worden ingetrokken.

5. De uitvoeringsbepalingen en IT-beveiligingsnormen die uit hoofde van Besluit C(2006) 3602 van 16 augustus 2006 zijn goedgekeurd, blijven, voor zover zij niet strijdig zijn met deze uitvoeringsbepalingen, van kracht totdat zij worden vervangen door de uit hoofde van artikel 13 van Besluit (EU, Euratom) 2017/46 vast te stellen uitvoeringsbepalingen en normen.

Artikel 11

Inwerkingtreding

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

Gedaan te Brussel, 6 april 2018.

Voor de Commissie,
namens de voorzitter,
Günther OETTINGER
Lid van de Commissie

BIJLAGE

TAKEN EN VERANTWOORDELIJKHEDEN (RASCI)

In het RASCI-model worden rollen aan entiteiten toegekend met de volgende afkortingen:

a) R — Responsible (verantwoordelijk)

b) A — Accountable (verantwoordingsplichtig)

c) S — Supporting (ondersteunend)

d) C — Consulted (geraadpleegd)

e) I — Informed (geïnformeerd)

Proces \ Rol	ISSB	HR (DS)	Afdelingen van de Commissie	Systeemeigenaar	Gegevenseigenaar	LISO	DIGIT	Contractanten
Aanpassing aan het informatiebeveiligingsbeleid van de Commissie		**R/A**	**S**				**S**	
Encryptietechnologie		**C**	**A**	**R**	**I**	**C**		
IT-beveiligingsinspecties	**I**	**A/R**		**S**	**I**	**I**	**S**	
Toegang via externe netwerken	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Uitbesteden van CIS'en		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] De ISSB wordt geraadpleegd met betrekking tot het gebruik van een intern netwerk door een andere afdeling van de Commissie dan het directoraat-generaal Informatica.

[2] De systeemeigenaar van een CIS dat wordt uitbesteed, is verantwoordelijk, en de systeemeigenaar van een ander CIS dat verbonden is met een uitbesteed CIS, moet worden geraadpleegd.