BESLUITEN

BESLUIT (EU, Euratom) 2017/46 VAN DE COMMISSIE

van 10 januari 2017

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,

Overwegende hetgeen volgt:

(1) De communicatie- en informatiesystemen van de Commissie zijn een integrerend onderdeel van de werking van de Commissie, en IT-beveiligingsincidenten kunnen ernstige gevolgen hebben voor de werkzaamheden van de Commissie, alsmede voor derden, waaronder natuurlijke personen, ondernemingen en lidstaten.

(2) Er bestaan vele dreigingen die de vertrouwelijkheid, integriteit of beschikbaarheid van de communicatie- en informatiesystemen van de Commissie en de daarin verwerkte gegevens kunnen aantasten. Deze dreigingen, die onder meer ongevallen, fouten, opzettelijke aanvallen en natuurverschijnselen omvatten, moeten als operationele risico's worden erkend.

(3) Communicatie- en informatiesystemen moeten zijn voorzien van bescherming op een niveau dat in overeenstemming is met de waarschijnlijkheid, het effect en de aard van de risico's waaraan zij zijn blootgesteld.

(4) De IT-beveiliging binnen de Commissie moet waarborgen dat de communicatie- en informatiesystemen van de Commissie de erin verwerkte gegevens beschermen en dat zij, wanneer zij door rechtmatige gebruikers worden bediend, op alle noodzakelijke momenten functioneren overeenkomstig wat noodzakelijk is.

(5) De tenuitvoerlegging van het IT-beveiligingsbeleid van de Commissie moet consistent zijn met die van het beleid dat binnen de Commissie op beveiligingsgebied wordt toegepast.

(6) De algemene verantwoordelijkheid voor de beveiliging binnen de Commissie berust bij het directoraat Beveiliging van het directoraat-generaal Personele Middelen en Veiligheid, onder het gezag en de verantwoordelijkheid van het met de beveiliging belaste lid van de Commissie.

(7) De door de Commissie gehanteerde benadering moet rekening houden met beleidsinitiatieven en wetgeving van de EU inzake netwerk- en informatiebeveiliging, industrienormen en goede praktijken, teneinde aan alle wetgeving ter zake te voldoen en interoperabiliteit en compatibiliteit mogelijk te maken.

(8) De voor de communicatie- en informatiesystemen verantwoordelijke afdelingen van de Commissie moeten passende maatregelen ontwikkelen en uitvoeren en de IT-beveiligingsmaatregelen ter bescherming van de communicatie- en informatiesystemen moeten binnen de Commissie worden gecoördineerd met het oog op efficiëntie en doeltreffendheid.

(9) De voorschriften en procedures voor de toegang tot informatie in de context van de IT-beveiliging, met inbegrip van de afhandeling van IT-beveiligingsincidenten, moeten evenredig zijn met de dreiging voor de Commissie en haar personeel en moeten voldoen aan de beginselen die zijn vastgelegd in Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad [1] betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de uniale instellingen en organen en betreffende het vrije verkeer van die gegevens, met inachtneming van de geheimhoudingsplicht bedoeld in artikel 339 VWEU.

[1] Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (PB L 8 van 12.1.2001, blz. 1).

(10) Het beleid en de voorschriften inzake communicatie- en informatiesystemen waarmee gerubriceerde EU-informatie (EUCI), gevoelige niet-gerubriceerde informatie en andere niet-gerubriceerde informatie wordt verwerkt, moeten volledig in overeenstemming zijn met Besluiten (EU, Euratom) 2015/443 ([1]) en (EU, Euratom) 2015/444 ([2]) van de Commissie.

(11) Het is noodzakelijk dat de Commissie de bepalingen inzake de beveiliging van de door de Commissie gebruikte communicatie- en informatiesystemen herziet en actualiseert.

(12) Besluit C(2006) 3602 van de Commissie dient bijgevolg te worden ingetrokken,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

HOOFDSTUK 1

ALGEMENE BEPALINGEN

Artikel 1

Onderwerp en toepassingsgebied

1. Dit besluit is van toepassing op alle communicatie- en informatiesystemen, hierna „CIS" genoemd, die in het bezit zijn van de Commissie of die door of namens de Commissie worden aangeschaft, beheerd of geëxploiteerd, en op elk gebruik van die CIS door de Commissie.

2. Bij dit besluit worden de fundamentele beginselen, doelstellingen, organisatie en verantwoordelijkheden betreffende de beveiliging van deze CIS bepaald, en in het bijzonder ten aanzien van afdelingen van de Commissie die in het bezit zijn van CIS dan wel deze aanschaffen, beheren of exploiteren, met inbegrip van CIS die door een interne IT-dienstverlener worden verstrekt. Wanneer op basis van een bilaterale overeenkomst met de Commissie een externe partij in het bezit is van een CIS of deze verstrekt, beheert of exploiteert, is dit besluit op de voorwaarden van die overeenkomst van toepassing.

3. Dit besluit is van toepassing op alle afdelingen van de Commissie en uitvoerende agentschappen. Wanneer op basis van een bilaterale overeenkomst met de Commissie een CIS van de Commissie wordt gebruikt door andere organen of instellingen, is dit besluit op de voorwaarden van die overeenkomst van toepassing.

4. Ongeacht mogelijke specifieke aanwijzingen met betrekking tot bepaalde categorieën personeel is dit besluit van toepassing op de leden van de Commissie, op het personeel van de Commissie als bedoeld in het Statuut van de ambtenaren van de Europese Unie (hierna „Statuut" genoemd) en de Regeling welke van toepassing is op de andere personeelsleden van de Europese Unie ([3]), op nationale deskundigen die bij de Commissie zijn gedetacheerd ([4]), op externe dienstverleners en hun personeel, op stagiairs en alle andere personen die toegang hebben tot CIS die onder dit besluit vallen.

5. Dit besluit is van toepassing op het Europees Bureau voor fraudebestrijding (OLAF) voor zover verenigbaar met de Uniewetgeving en met Besluit 1999/352/EG, EGKS, Euratom van de Commissie ([5]). In het bijzonder zijn de maatregelen waarin dit besluit voorziet, met inbegrip van instructies, inspecties, onderzoeken en gelijkwaardige maatregelen, mogelijk niet van toepassing op CIS van de Commissie indien de toepassing onverenigbaar is met de onafhankelijkheid van het onderzoek van OLAF en/of de geheimhouding van informatie die door OLAF bij het uitvoeren daarvan is verkregen.

Artikel 2

Definities

In dit besluit wordt verstaan onder:

1. „verantwoordingsplicht": de verplichting om verantwoording af te leggen met betrekking tot acties, besluiten en prestaties;

([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).

([2]) Besluit (EU, Euratom) 2015/444 van de Commissie van 13 maart 2015 betreffende de veiligheidsvoorschriften voor de bescherming van gerubriceerde EU-informatie (PB L 72van 17.3.2015, blz. 53).

([3]) Vastgesteld bij Verordening (EEG, Euratom, EGKS) nr. 259/68 van de Raad van 29 februari 1968 tot vaststelling van het Statuut van de ambtenaren van de Europese Gemeenschappen en de regeling welke van toepassing is op de andere personeelsleden van deze Gemeenschappen, alsmede van bijzondere maatregelen welke tijdelijk op de ambtenaren van de Commissie van toepassing zijn (Regeling welke van toepassing is op de andere personeelsleden van de Europese Unie) (PB L 56 van 4.3.1968, blz. 1).

([4]) Besluit van de Commissie van 12 november 2008 houdende voorschriften betreffende de detachering bij de Commissie van nationale deskundigen en nationale deskundigen in opleiding (C(2008) 6866 final).

([5]) 1999/352/EG, EGKS, Euratom: Besluit van de Commissie van 28 april 1999 houdende oprichting van het Europees Bureau voor fraudebestrijding (OLAF) (PB L 136 van 31.5.1999, blz. 20).

2. „CERT-EU": het computercrisisteam voor de EU-instellingen en agentschappen. CERT-EU heeft tot taak de Europese instellingen te ondersteunen bij de bescherming tegen doelbewuste en kwaadwillige aanvallen die de integriteit van de IT-installaties kunnen aantasten en de belangen van de EU kunnen schaden. Tot de activiteiten van CERT-EU behoren preventie, opsporing, respons en herstel;

3. „afdeling van de Commissie" een directoraat-generaal of dienst van de Commissie, of een kabinet van een lid van de Commissie;

4. „Veiligheidsautoriteit van de Commissie": de in Besluit 2015/444 (EU, Euratom) bedoelde functie;

5. „communicatie- en informatiesysteem" of „CIS": elk systeem dat de verwerking van informatie in elektronische vorm mogelijk maakt, met inbegrip van alle daarvoor vereiste goederen, infrastructuur, organisatie, personeel en informatiebronnen. Deze definitie omvat tevens zakelijke toepassingen, gedeelde IT-diensten, uitbestede systemen en eindgebruikersapparatuur;

6. „bestuursraad" of „CMB": de instantie die instaat voor het hoogste niveau van managementtoezicht inzake operationele en bestuurlijke aangelegenheden binnen de Commissie;

7. „gegevenseigenaar": de persoon die ervoor verantwoordelijk is dat wordt voorzien in de bescherming en het gebruik van een specifieke dataset door een CIS;

8. „dataset": een reeks gegevens die ten dienste staat van een specifiek bedrijfsproces of een specifieke bedrijfsactiviteit van de Commissie;

9. „noodprocedure": een vooraf vastgestelde reeks methoden en verantwoordelijkheden die in spoedeisende situaties worden toegepast om ernstige gevolgen voor de Commissie te voorkomen;

10. „beleid inzake informatiebeveiliging": een verzameling doelstellingen op het gebied van informatiebeveiliging die moeten worden vastgesteld, uitgevoerd en geverifieerd. Hiertoe behoren onder meer de Besluiten (EU, Euratom) 2015/443 en (EU, Euratom) 2015/444;

11. „stuurgroep voor informatiebeveiliging" of „ISSB": een governanceorgaan dat de bestuursraad ondersteunt bij taken die met IT-beveiliging samenhangen;

12. „interne IT-dienstverlener": een afdeling van de Commissie die gedeelde IT-diensten verleent;

13. „IT-beveiliging" of „beveiliging van communicatie- en informatiesystemen" of „beveiliging van CIS": de instandhouding van de vertrouwelijkheid, de integriteit en de beschikbaarheid van communicatie- en informatiesystemen en de datasets die erin worden verwerkt;

14. „richtsnoeren voor IT-beveiliging": aanbevolen, maar vrijwillige maatregelen die de ondersteuning van IT-beveiligingsnormen vergemakkelijken of als referentie dienen bij gebreke van een toepasselijke norm;

15. „IT-beveiligingsincident": een gebeurtenis die de vertrouwelijkheid, de integriteit of de beschikbaarheid van een CIS nadelig zou kunnen beïnvloeden;

16. „IT-beveiligingsmaatregel": een technische of organisatorische maatregel gericht op beperking van IT-beveiligingsrisico's;

17. „noodzaak van IT-beveiliging": een precieze en ondubbelzinnige bepaling van het bij een gegeven of een IT-systeem behorende niveau van vertrouwelijkheid, integriteit en beschikbaarheid, bedoeld om de vereiste mate van bescherming vast te stellen;

18. „IT-beveiligingsdoelstelling": een verklaring van de intentie om welbepaalde dreigingen het hoofd te bieden en/of te voldoen aan welbepaalde organisatorische beveiligingsvereisten of -aannames;

19. „IT-beveiligingsplan": de documentatie van de IT-beveiligingsmaatregelen die vereist zijn om aan de noodzaak van IT-beveiliging in verband met een communicatie- en informatiesysteem te voldoen;

20. „IT-beveiligingsbeleid": een verzameling doelstellingen op het gebied van IT-beveiliging die moeten worden vastgesteld, uitgevoerd en geverifieerd. Het IT-beveiligingsbeleid omvat dit besluit en de uitvoeringsbepalingen ervoor;

21. „IT-beveiligingsvereiste": een volgens een vooraf bepaald proces geformaliseerde noodzaak van IT-beveiliging;

22. „IT-beveiligingsrisico": het gevolg dat een IT-beveiligingsdreiging voor een communicatie- en informatiesysteem kan hebben door een kwetsbaarheid van dat systeem te exploiteren. Een IT-beveiligingsrisico wordt dus gekenmerkt door twee factoren: 1) onzekerheid, dat wil zeggen de kans dat een IT-beveiligingsdreiging tot een ongewenste gebeurtenis leidt, en 2) impact, dat wil zeggen de gevolgen die voor een communicatiesysteem uit deze ongewenste gebeurtenis kunnen voortvloeien;

23. „IT-beveiligingsnormen": specifieke verplichte IT-beveiligingsmaatregelen die bijdragen tot de handhaving en ondersteuning van het IT-beveiligingsbeleid;

24. „IT-beveiligingsstrategie": een reeks projecten en activiteiten die zijn opgezet om de doelstellingen van de Commissie te bereiken en die moeten worden vastgesteld, uitgevoerd en geverifieerd;

25. „IT-beveiligingsdreiging": een factor die mogelijk een ongewenste gebeurtenis tot gevolg heeft die tot schade aan een communicatie- en informatiesysteem kan leiden. Dergelijke dreigingen kunnen opzettelijk of onopzettelijk zijn en worden gekenmerkt door bedreigende elementen, mogelijke doelwitten en aanvalsmethoden;

26. „plaatselijke informaticabeveiligingsfunctionaris" of „LISO": de verbindingsfunctionaris op het gebied van IT-beveiliging voor een afdeling van de Commissie;

27. de termen „persoonsgegevens", „verwerking van persoonsgegevens", „verwerkingsverantwoordelijke" en „bestand van persoonsgegevens" hebben dezelfde betekenis als de termen „persoonsgegevens", „verwerking van persoonsgegevens", „verantwoordelijke voor de verwerking" en „bestand van persoonsgegevens" in Verordening (EG) nr. 45/2001, en met name artikel 2;

28. „verwerking van informatie": alle functies van een communicatie- en informatiesysteem met betrekking tot datasets, waaronder het aanmaken, het wijzigen, het weergeven, het opslaan, het doorgeven, het wissen en het archiveren van informatie. De verwerking van informatie kan door een communicatie- en informatiesysteem worden aangeboden als een functie voor de gebruikers of een IT-dienst voor andere communicatie- en informatiesystemen;

29. „geheimhouding": de bescherming van bedrijfsgegevens die naar hun aard vallen onder de geheimhoudingsplicht en met name de inlichtingen betreffende ondernemingen en hun handelsbetrekkingen of bestanddelen van hun kostprijzen, zoals bedoeld in artikel 339 VWEU;

30. „verantwoordelijk": de verplichting hebbend om op te treden en besluiten te nemen om de vereiste resultaten tot stand te brengen;

31. „beveiliging binnen de Commissie": de beveiliging van personen, goederen en informatie binnen de Commissie, en meer specifiek de fysieke integriteit van personen en goederen, de integriteit, vertrouwelijkheid en beschikbaarheid van informatie en communicatie- en informatiesystemen, alsook het onbelemmerde functioneren van de werkzaamheden van de Commissie;

32. „gedeelde IT-dienst": een dienst die een communicatie- en informatiesysteem verstrekt aan andere communicatie- en informatiesystemen op het gebied van de verwerking van informatie;

33. „systeemeigenaar": de persoon die de algehele verantwoordelijkheid draagt voor de aanschaf, ontwikkeling, integratie, wijziging, werking, onderhoud en buitendienststelling van een communicatie- en informatiesysteem;

34. „gebruiker": een persoon die gebruikmaakt van de functies die een communicatie- en informatiesysteem aanbiedt, zowel binnen als buiten de Commissie.

Artikel 3

Beginselen van IT-beveiliging binnen de Commissie

1. De IT-beveiliging binnen de Commissie is gegrondvest op de beginselen van wettelijkheid, transparantie, evenredigheid en verantwoordingsplicht.

2. Bij de ontwikkeling en tenuitvoerlegging van de communicatie- en informatiesystemen van de Commissie wordt van bij de aanvang rekening gehouden met IT-beveiligingsvraagstukken. Met het oog daarop wordt voorzien in de medewerking, elk op zijn verantwoordelijkheidsgebied, van het directoraat-generaal Informatica en het directoraat-generaal Personele Middelen en Veiligheid.

3. Effectieve IT-beveiliging houdt in dat de volgende aspecten op passende wijze worden gewaarborgd:

a) authenticiteit: de garantie dat informatie echt is en van bonafide bronnen afkomstig is;

b) beschikbaarheid: de eigenschap dat informatie op verzoek van een gemachtigde entiteit toegankelijk en bruikbaar is;

c) vertrouwelijkheid: de eigenschap dat informatie niet wordt vrijgegeven aan niet-gemachtigde personen, entiteiten of processen;

d) integriteit: de eigenschap dat de nauwkeurigheid en de volledigheid van de goederen en de informatie is gewaarborgd;

e) onweerlegbaarheid: de eigenschap dat kan worden bewezen dat een actie of gebeurtenis heeft plaatsgevonden, zodat deze actie of gebeurtenis niet achteraf kan worden ontkend;

f) bescherming van persoonsgegevens: het voorzien in passende waarborgen ten aanzien van persoonsgegevens, met volledige inachtneming van Verordening (EG) nr. 45/2001:

g) geheimhouding: de bescherming van informatie die naar haar aard onder de geheimhoudingsplicht valt en met name inlichtingen betreffende ondernemingen en hun handelsbetrekkingen of de bestanddelen van hun kostprijzen, zoals bedoeld in artikel 339 VWEU;

4. De IT-beveiliging is op een risicobeheersingsprocedure gebaseerd. Het doel van dit proces is het niveau van de IT-beveiligingsrisico's te bepalen en beveiligingsmaatregelen vast te stellen teneinde deze risico's tegen redelijke kosten tot een aanvaardbaar niveau terug te brengen.

5. Alle communicatie- en informatiesystemen worden geïdentificeerd, aan een systeemeigenaar toegewezen en in een inventaris geregistreerd.

6. De beveiligingsvereisten van elk communicatie- en informatiesysteem worden vastgesteld op basis van de noodzaak van beveiliging ervan en de noodzaak van beveiliging van de erin verwerkte informatie. Communicatie- en informatiesystemen die diensten verlenen aan andere communicatie- en informatiesystemen kunnen worden ontworpen zodat zij welbepaalde niveaus van noodzaak van beveiliging ondersteunen.

7. De IT-beveiligingsplannen en IT-beveiligingsmaatregelen zijn evenredig met de noodzaak van beveiliging van de communicatie- en informatiesystemen.

De processen die met deze beginselen en activiteiten samenhangen, worden in uitvoeringsbepalingen nader uitgewerkt.

HOOFDSTUK 2

ORGANISATIE EN VERANTWOORDELIJKHEDEN

Artikel 4

Bestuursraad

De bestuursraad wordt belast met de algemene verantwoordelijkheid voor het beheer van alle IT-beveiliging binnen de Commissie.

Artikel 5

Stuurgroep voor informatiebeveiliging (ISSB)

1. Het voorzitterschap van de ISSB wordt bekleed door de adjunct-secretaris-generaal die verantwoordelijk is voor het beheer van de IT-beveiliging binnen de Commissie. De leden van de ISSB vertegenwoordigen zakelijke, technologische en beveiligingsbelangen in de afdelingen van de Commissie en omvatten vertegenwoordigers van het directoraat-generaal Informatica, het directoraat-generaal Personele Middelen en Veiligheid, het directoraat-generaal Begroting en, bij toerbeurt gedurende twee jaar, vertegenwoordigers van vier andere betrokken afdelingen van de Commissie voor de activiteiten waarvan IT-beveiliging een belangrijke factor is. De leden maken deel uit van het hogere management.

2. De ISSB ondersteunt de bestuursraad bij zijn taken op het gebied van IT-beveiliging. De ISSB wordt belast met de operationele verantwoordelijkheid voor het beheer van alle IT-beveiliging binnen de Commissie.

3. De ISSB doet aanbevelingen aan de Commissie voor het IT-beveiligingsbeleid van de Commissie.

4. De ISSB evalueert beheersvraagstukken en vraagstukken die met IT-beveiliging samenhangen, met inbegrip van ernstige IT-beveiligingsincidenten, en brengt daarover halfjaarlijks verslag uit aan de bestuursraad.

5. DE ISSB monitort en evalueert de algemene uitvoering van dit besluit en brengt daarover verslag uit aan de bestuursraad.

6. Op voorstel van het directoraat-generaal Informatica evalueert en monitort de ISSB de uitvoering van de doorlopende IT-beveiligingsstrategie en keurt zij deze goed. De ISSB brengt daarover verslag uit aan de bestuursraad.

7. De ISSB monitort, evalueert en controleert de situatie op het gebied van de behandeling van bedrijfsinformatierisico's en is bevoegd formele vereisten vast te stellen inzake noodzakelijke verbeteringen.

De processen die met deze verantwoordelijkheden en activiteiten samenhangen, worden in uitvoeringsbepalingen nader uitgewerkt.

Artikel 6

Directoraat-generaal Personele Middelen en Veiligheid

Ten aanzien van IT-beveiliging heeft het directoraat-generaal Personele Middelen en Veiligheid de hierna omschreven verantwoordelijkheden. Het directoraat-generaal:

1. zorgt voor de onderlinge aanpassing van het IT-beveiligingsbeleid en het informatiebeveiligingsbeleid van de Commissie;

2. stelt een kader in voor het verlenen van toestemming voor het gebruik van encryptietechnologieën voor de opslag en transmissie van informatie door communicatie- en informatiesystemen;

3. licht het directoraat-generaal Informatica in over specifieke dreigingen die significante gevolgen zouden kunnen hebben voor de beveiliging van de communicatie- en informatiesystemen en de daarin verwerkte gegevens;

4. voert IT-beveiligingsinspecties uit ter beoordeling van de conformiteit van de communicatie- en informatiesystemen van de Commissie met het beveiligingsbeleid, en brengt over de resultaten verslag uit aan de ISSB;

5. stelt een kader in voor het verlenen van de bevoegdheid om vanuit externe netwerken toegang te krijgen tot communicatie- en informatiesystemen van de Commissie en het vaststellen van passende beveiligingsvoorschriften daarvoor, en ontwikkelt de daarmee samenhangende IT-beveiligingsnormen en -richtsnoeren in nauwe samenwerking met het directoraat-generaal Informatica;

6. stelt beginselen en voorschriften inzake de uitbesteding van communicatie- en informatiesystemen voor, teneinde passende controle over de beveiliging van de informatie te behouden;

7. ontwikkelt IT-beveiligingsnormen en -richtsnoeren met betrekking tot artikel 6, in nauwe samenwerking met het directoraat-generaal Informatica.

De processen die met deze verantwoordelijkheden en activiteiten samenhangen, worden in uitvoeringsbepalingen nader uitgewerkt.

Artikel 7

Directoraat-generaal Informatica

Ten aanzien van de algehele IT-beveiliging in de Commissie heeft het directoraat-generaal Informatica de hierna omschreven verantwoordelijkheden. Het directoraat-generaal:

1. ontwikkelt IT-beveiligingsnormen en -richtsnoeren, behoudens het bepaalde in artikel 6, in nauwe samenwerking met het directoraat-generaal Personele Middelen en Veiligheid, teneinde de consistentie van het IT-beveiligingsbeleid en het informatiebeveiligingsbeleid van de Commissie te verzekeren, en doet daaromtrent voorstellen aan de ISSB;

2. beoordeelt de methoden, processen en resultaten inzake IT-beveiligingsrisicobeheersing van alle afdelingen van de Commissie en brengt daarover regelmatig verslag uit aan de ISSB;

3. stelt een doorlopende IT-beveiligingsstrategie voor, die ter herziening en goedkeuring aan de ISSB wordt voorgelegd en met het oog op formele vaststelling bij de bestuursraad wordt ingediend, en stelt een programma en een planning van projecten en activiteiten ter uitvoering van de IT-beveiligingsstrategie voor;

4. monitort de uitvoering van de IT-beveiligingsstrategie van de Commissie en brengt daarover regelmatig verslag uit aan de ISSB;

5. monitort de IT-beveiligingsrisico's en de IT-beveiligingsmaatregelen die in de communicatie- en informatiesystemen zijn geïmplementeerd, en brengt daarover regelmatig verslag uit aan de ISSB;

6. brengt aan de ISSB regelmatig verslag uit over de algehele uitvoering en naleving van dit besluit;

7. verzoekt systeemeigenaars, na overleg met het directoraat-generaal Personele Middelen en Veiligheid, om specifieke IT-beveiligingsmaatregelen te nemen teneinde IT-beveiligingsrisico's voor de communicatie- en informatiesystemen van de Commissie te reduceren;

8. zorgt ervoor dat systeemeigenaars en gegevenseigenaars kunnen beschikken over een passende catalogus van door het directoraat-generaal Informatica aangeboden IT-beveiligingsdiensten, zodat zij hun verantwoordelijkheden op het gebied van IT-beveiliging kunnen vervullen en het IT-beveiligingsbeleid en de IT-beveiligingsnormen kunnen naleven;

9. verstrekt systeemeigenaars en gegevenseigenaars passende documentatie en overlegt zo nodig met hen over de IT-beveiligingsmaatregelen die voor hun IT-diensten zijn getroffen teneinde de naleving van het IT-beveiligingsbeleid te faciliteren en de systeemeigenaars te ondersteunen op het gebied van IT-risicobeheersing;

10. organiseert regelmatige bijeenkomsten van het LISO-netwerk en ondersteunt de LISO's bij de uitvoering van hun taken;

11. stelt de opleidingsbehoeften vast en coördineert de opleidingsprogramma's op het gebied van IT-beveiliging in samenwerking met de afdelingen van de Commissie, en zorgt in samenwerking met het directoraat-generaal Personele Middelen en Veiligheid voor de ontwikkeling, uitvoering en coördinatie van bewustmakingscampagnes inzake IT-beveiliging;

12. zorgt ervoor dat systeemeigenaars, gegevenseigenaars en andere functies met verantwoordelijkheden op het gebied van IT-beveiliging binnen de afdelingen van de Commissie bekend zijn met het IT-beveiligingsbeleid;

13. licht het directoraat-generaal Personele Middelen en Veiligheid in over specifieke IT-beveiligingsdreigingen en -incidenten en uitzonderingen op het IT-beveiligingsbeleid van de Commissie die door de systeemeigenaars zijn gemeld en een significant effect zouden kunnen hebben op de beveiliging binnen de Commissie;

14. verstrekt de Commissie, met betrekking tot zijn taak als interne verlener van IT-diensten, een catalogus van gedeelde IT-diensten die welbepaalde beveiligingsniveaus bieden. Dit gebeurt door de IT-beveiligingsrisico's stelselmatig te beoordelen, te beheren en te monitoren met het oog op de uitvoering van de beveiligingsmaatregelen die nodig zijn om het vastgestelde beveiligingsniveau te verwezenlijken.

De processen en nader gedetailleerde verantwoordelijkheden worden in uitvoeringsbepalingen nader uitgewerkt.

Artikel 8

Afdelingen van de Commissie

De hoofden van alle afdelingen van de Commissie, wat de IT-beveiliging betreft:

1. wijzen voor elk communicatie- en informatiesysteem formeel een ambtenaar of tijdelijke functionaris aan als systeemeigenaar, die verantwoordelijk is voor de IT-beveiliging van dat communicatie- en informatiesysteem, en wijzen voor elke in een communicatie- en informatiesysteem verwerkte dataset een gegevenseigenaar aan, die behoort tot dezelfde administratieve entiteit die de verwerkingsverantwoordelijke is voor datasets waarop Verordening (EG) nr. 45/2001 van toepassing is;

2. wijzen formeel een plaatselijke informaticabeveiligingsfunctionaris (LISO) aan, die de desbetreffende verantwoordelijkheden onafhankelijk van de systeemeigenaar en de gegevenseigenaar kan uitvoeren. Een LISO kan worden aangewezen voor één of meer afdelingen van de Commissie;

3. zorgen ervoor dat passende IT-beveiligingsrisicobeoordelingen en IT-beveiligingsplannen zijn opgesteld en uitgevoerd;

4. zorgen ervoor dat een het directoraat-generaal Informatica op regelmatige basis een overzicht krijgt van de IT-beveiligingsrisico's en IT-beveiligingsmaatregelen;

5. zorgen met de steun van het directoraat-generaal Informatica ervoor dat er passende processen, procedures en oplossingen zijn om IT-beveiligingsrisico's met betrekking tot hun communicatie- en informatiesystemen efficiënt op te sporen, te rapporteren en op te lossen;

6. starten een noodprocedure op bij IT-beveiligingsnoodgevallen;

7. hebben de uiteindelijke verantwoordingsplicht voor de IT-beveiliging, met inbegrip van de verantwoordelijkheden van de systeemeigenaar en de gegevenseigenaar;

8. zijn eigenaar van de risico's met betrekking tot hun communicatie- en informatiesystemen en datasets;

9. zorgen ervoor dat meningsverschillen tussen gegevenseigenaars en systeemeigenaars worden opgelost, en leggen aanhoudende meningsverschillen aan de ISSB voor;

10. zorgen ervoor dat de IT-beveiligingsplannen en IT-beveiligingsmaatregelen worden uitgevoerd en dat de risico's naar behoren zijn gedekt.

De processen die met deze verantwoordelijkheden en activiteiten samenhangen, worden in uitvoeringsbepalingen nader uitgewerkt.

Artikel 9

Systeemeigenaars

1. De systeemeigenaar is verantwoordelijk voor de IT-beveiliging van het communicatie- en informatiesysteem en brengt verslag uit aan het hoofd van de afdeling van de Commissie.

2. De systeemeigenaar doet op het gebied van IT-beveiliging het volgende:

a) hij zorgt voor de conformiteit van het communicatie- en informatiesysteem met het IT-beveiligingsbeleid;

b) hij zorgt ervoor dat het communicatie- en informatiesysteem naar behoren in de desbetreffende inventaris is opgenomen;

c) hij beoordeelt de IT-beveiligingsrisico's en stelt de noodzaak van IT-beveiliging vast in samenwerking met de gegevenseigenaars en in overleg met het directoraat-generaal Informatica;

d) hij stelt een beveiligingsplan op eventueel met gegevens over de beoordeelde risico's en vereiste aanvullende beveiligingsmaatregelen;

e) hij voert passende IT-beveiligingsmaatregelen uit die evenredig zijn aan de vastgestelde IT-beveiligingsrisico's en volgt de aanbevelingen die door de ISSB zijn goedgekeurd;

f) hij stelt eventuele afhankelijkheden van andere communicatie- en informatiesystemen of gedeelde IT-diensten vast en voert passende beveiligingsmaatregelen uit op basis van het beveiligingsniveau dat voor die communicatie- en informatiesystemen of gedeelde IT-diensten wordt voorgesteld;

g) hij beheert en monitort IT-beveiligingsrisico's;

h) hij brengt regelmatig verslag uit aan het hoofd van de afdeling van de Commissie over het IT-beveiligingsrisicoprofiel van zijn communicatie- en informatiesysteem en aan het directoraat-generaal Informatica over de daarmee samenhangende risico's, risicobeheersingsactiviteiten en beveiligingsmaatregelen;

i) hij raadpleegt de LISO van de betrokken afdeling van de Commissie inzake aspecten van IT-beveiliging;

j) hij geeft instructies aan de gebruikers over het gebruik van de communicatie- en informatiesystemen en de daarmee verband houdende gegevens en over de verantwoordelijkheden van de gebruikers met betrekking tot de communicatie- en informatiesystemen;

k) hij verzoekt het directoraat-generaal Personele Middelen en Veiligheid, dat als crypto-autoriteit optreedt, om toestemming voor elk communicatie- en informatiesysteem dat van encryptietechnologie gebruikmaakt;

l) hij raadpleegt vooraf de Veiligheidsautoriteit van de Commissie over elk systeem waarmee gerubriceerde EU-informatie wordt verwerkt;

m) hij zorgt ervoor dat alle encryptiesleutels in een escrowaccount worden opgeslagen. Versleutelde gegevens mogen slechts worden gerecupereerd wanneer daartoe toestemming is verleend overeenkomstig het door het directoraat-generaal Personele Middelen en Veiligheid vastgestelde kader;

n) hij volgt alle instructies van de betrokken verwerkingsverantwoordelijke op met betrekking tot de bescherming van persoonsgegevens en de toepassing van de gegevensbeschermingsregels ten aanzien van de beveiliging van de verwerking;

o) hij licht het directoraat-generaal Informatica in over elke uitzondering op het IT-beveiligingsbeleid van de Commissie, met vermelding van de reden daarvan;

p) hij stelt het hoofd van de afdeling van de Commissie op de hoogte van alle onoplosbare meningsverschillen tussen de gegevenseigenaar en de systeemeigenaar en meldt alle IT-beveiligingsincidenten tijdig aan de belanghebbenden in overeenstemming met de ernst ervan, zoals bepaald in artikel 15;

q) hij zorgt er ten aanzien van uitbestede systemen voor dat in het uitbestedingscontract passende IT-beveiligingsbepalingen zijn opgenomen en dat IT-beveiligingsincidenten met betrekking tot het uitbestede communicatie- en informatiesysteem overeenkomstig artikel 15 worden gemeld;

r) hij zorgt ten aanzien van communicatie- en informatiesystemen die gedeelde IT-diensten leveren, ervoor dat in een welbepaald, duidelijk gedocumenteerd beveiligingsniveau wordt voorzien en dat voor die communicatie- en informatiesystemen beveiligingsmaatregelen zijn geïmplementeerd die toereikend zijn om het bepaalde beveiligingsniveau te verwezenlijken.

3. Systeemeigenaars mogen een of meer van hun IT-beveiligingstaken formeel delegeren, maar blijven verantwoordelijk voor de IT-beveiliging van hun communicatie- en informatiesysteem.

De processen die met deze verantwoordelijkheden en activiteiten samenhangen, worden in uitvoeringsbepalingen nader uitgewerkt.

Artikel 10

Gegevenseigenaars

1. Gegevenseigenaars zijn jegens het hoofd van de afdeling van de Commissie verantwoordelijk voor de IT-beveiliging van een specifieke dataset en zijn aansprakelijk voor de vertrouwelijkheid, integriteit en beschikbaarheid van de dataset.

2. De gegevenseigenaar doet met betrekking tot deze dataset het volgende:

a) hij zorgt ervoor dat alle onder zijn verantwoordelijkheid vallende datasets naar behoren worden gerubriceerd overeenkomstig Besluiten (EU, Euratom) 2015/443 en (EU, Euratom) 2015/444;

b) hij stelt de noodzaak van informatiebeveiliging vast en licht de desbetreffende systeemeigenaars in over die noodzaak;

c) hij neemt deel aan de risicobeoordeling ten aanzien van communicatie- en informatiesystemen;

d) hij stelt het hoofd van de afdeling van de Commissie op de hoogte van alle onoplosbare meningsverschillen tussen de gegevenseigenaar en de systeemeigenaar;

e) hij meldt IT-beveiligingsincidenten overeenkomstig artikel 15.

3. Gegevenseigenaars mogen een of meer van hun IT-beveiligingstaken formeel delegeren, maar zij behouden de in dit artikel vastgestelde verantwoordelijkheden.

De processen die met deze verantwoordelijkheden en activiteiten samenhangen, worden in uitvoeringsbepalingen nader uitgewerkt.

Artikel 11

Plaatselijke informaticabeveiligingsfunctionarissen (LISO's)

De LISO doet op het gebied van IT-beveiliging het volgende:

a) hij bepaalt en informeert systeemeigenaars, gegevenseigenaars en andere functies met verantwoordelijkheden op het gebied van IT-beveiliging binnen de afdelingen van de Commissie proactief over het IT-beveiligingsbeleid;

b) als lid van het LISO-netwerk onderhoudt hij contacten met het directoraat-generaal Informatica met betrekking tot kwesties die binnen de afdelingen van de Commissie onder het IT-beveiligingsbeleid vallen;

c) hij woont de regelmatige LISO-vergaderingen bij;

d) hij houdt het proces van risicobeheersing op het gebied van informatiebeveiliging en de ontwikkeling en tenuitvoerlegging van beveiligingsplannen voor informatiesystemen in het oog;

e) hij adviseert gegevenseigenaars, systeemeigenaars en hoofden van afdelingen van de Commissie over kwesties in verband met IT-beveiliging;

f) hij verspreidt in samenwerking met het directoraat-generaal Informatica goede IT-praktijken en stelt specifieke bewustmakings- en opleidingsprogramma's voor;

g) hij brengt verslag uit over IT-beveiliging en licht het hoofd van de afdeling van de Commissie in over tekortkomingen en verbeteringen.

De processen die met deze verantwoordelijkheden en activiteiten samenhangen, worden in uitvoeringsbepalingen nader uitgewerkt.

Artikel 12

Gebruikers

1. Gebruikers doen op het gebied van IT-beveiliging het volgende:

a) zij houden zich aan het IT-beveiligingsbeleid en de instructies van de systeemeigenaar over het gebruik van elk communicatie- en informatiesysteem;

b) zij melden IT-beveiligingsincidenten overeenkomstig artikel 15.

2. Het gebruik van communicatie- en informatiesystemen van de Commissie in strijd met het IT-beveiligingsbeleid of de instructies van de systeemeigenaar kan aanleiding geven tot een tuchtrechtelijke procedure.

De processen die met deze verantwoordelijkheden en activiteiten samenhangen, worden in uitvoeringsbepalingen nader uitgewerkt.

HOOFDSTUK 3

VEREISTEN EN VERPLICHTINGEN OP HET GEBIED VAN BEVEILIGING

Artikel 13

Uitvoering van dit besluit

1. De uitvoeringsbepalingen voor artikel 6 en de daarmee verband houdende normen en richtsnoeren worden vastgesteld door middel van een machtigingsbesluit van de Commissie ten behoeve van het lid van de Commissie dat bevoegd is voor veiligheidszaken.

2. Alle andere uitvoeringsbepalingen met betrekking tot dit besluit en de daarmee verband houdende normen en richtsnoeren worden vastgesteld door middel van een machtigingsbesluit van de Commissie ten behoeve van het lid van de Commissie dat bevoegd is voor informatica.

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

Artikel 14

Verplichting tot naleving

1. De naleving van de in het IT-beveiligingsbeleid en de IT-beveiligingsnormen vastgelegde bepalingen is verplicht.

2. Niet-naleving van het IT-beveiligingsbeleid en de IT-beveiligingsnormen kan tuchtrechtelijke maatregelen tot gevolg hebben overeenkomstig de Verdragen, het Statuut en de Regeling welke van toepassing is op de andere personeelsleden van de Europese Unie, alsook contractuele sancties en/of gerechtelijke stappen overeenkomstig de nationale wet- en regelgeving.

3. Het directoraat-generaal Informatica wordt ingelicht over elke uitzondering op het IT-beveiligingsbeleid.

4. Indien de ISSB van oordeel is dat er een aanhoudend onaanvaardbaar risico voor een communicatie- en informatiesysteem van de Commissie bestaat, stelt het directoraat-generaal Informatie in samenwerking met de systeemeigenaar risicobeperkende maatregelen voor aan de ISSB. Die maatregelen kunnen onder meer versterkte monitoring en verslaglegging alsmede beperking van de dienstverlening en afsluiting van het communicatie- en informatiesysteem inhouden.

5. De ISSB geeft zo nodig opdracht tot de uitvoering van de goedgekeurde risicobeperkende maatregelen. De ISSB kan tevens aanbevelen dat de directeur-generaal van het directoraat-generaal Personele Middelen en Veiligheid een administratief onderzoek opent. Het directoraat-generaal Informatica brengt aan de ISSB verslag uit over elke situatie waarin opdracht tot uitvoering van risicobeperkende maatregelen wordt gegeven.

De processen die met deze verantwoordelijkheden en activiteiten samenhangen, worden in uitvoeringsbepalingen nader uitgewerkt.

Artikel 15

Behandeling van IT-beveiligingsincidenten

1. Het directoraat-generaal Informatica is verantwoordelijk voor het verzekeren van de belangrijkste operationele responscapaciteit bij IT-beveiligingsincidenten binnen de Europese Commissie.

2. Voor het directoraat-generaal Personele Middelen en Veiligheid als meewerkende belanghebbende bij de respons op IT-beveiligingsincidenten geldt het volgende:

a) het heeft recht op toegang tot samenvattende informatie over alle incidenten en op verzoek tot de volledige dossiers;

b) het neemt deel aan crisisbeheersingsgroepen inzake IT-beveiligingsincidenten en aan noodprocedures inzake IT-beveiliging;

c) het is belast met de betrekkingen met de rechtshandhavings- en inlichtingendiensten;

d) het voert overeenkomstig artikel 11 van Besluit (EU, Euratom) 2015/443 forensische analyses uit met betrekking tot cyberbeveiliging;

e) het beslist over de noodzaak om een formeel onderzoek in te stellen;

f) het licht het directoraat-generaal Informatica in over elk IT-beveiligingsincident dat een risico voor andere communicatie- en informatiesystemen kan inhouden.

3. Het directoraat-generaal Informatica en het directoraat-generaal Personele Middelen en Veiligheid houden regelmatig contact met het oog op de uitwisseling van informatie en de coördinatie van de behandeling van beveiligingsincidenten, met name ten aanzien van elk IT-beveiligingsincident waarvoor een formeel onderzoek vereist kan zijn.

4. De coördinatiediensten voor incidenten van het computercrisisresponsteam van de Europese instellingen, organen en agentschappen (CERT-EU) kunnen indien nodig worden ingezet ter ondersteuning van het proces van incidentenbehandeling en voor het delen van informatie met eventuele andere getroffen EU-instellingen en agentschappen.

5. Systeemeigenaars die bij een IT-beveiligingsincident zijn betrokken, doen het volgende:

a) zij lichten bij elk belangrijk IT-beveiligingsincident, met name indien er sprake is van een inbreuk op de vertrouwelijkheid van de gegevens, onmiddellijk het hoofd van hun afdeling van de Commissie, het directoraat-generaal Informatica, het directoraat-generaal Personele Middelen en Veiligheid, de LISO en indien van toepassing de gegevenseigenaar in;

b) zij volgen de instructies van de bevoegde autoriteiten van de Commissie inzake mededeling, respons en herstel in geval van incident en verlenen daaraan hun medewerking.

6. Gebruikers melden elk feitelijk of vermoed IT-beveiligingsincident tijdig aan de bevoegde IT-helpdesk.

7. Gegevenseigenaars melden elk feitelijk of vermoed IT-beveiligingsincident tijdig aan het bevoegde responsteam voor IT-beveiligingsincidenten.

8. Het directoraat-generaal Informatica, ondersteund door de andere bijdragende belanghebbenden, is verantwoordelijk voor de behandeling van elk geconstateerd IT-beveiligingsincident met betrekking tot communicatie- en informatiesystemen van de Commissie die geen uitbesteed systeem zijn.

9. Het directoraat-generaal Informatica licht de getroffen afdelingen van de Commissie, de bevoegde LISO's en waar van toepassing CERT-EU in over IT-beveiligingsincidenten, indien er sprake is van een noodzaak tot kennisneming.

10. Het directoraat-generaal Informatica brengt aan de ISSB regelmatig verslag uit over belangrijke IT-beveiligingsincidenten waarbij communicatie- en informatiesystemen van de Commissie betrokken zijn.

11. De bevoegde LISO heeft op verzoek toegang tot dossiers betreffende IT-beveiligingsincidenten waarbij communicatie- en informatiesystemen van de Commissie betrokken zijn.

12. Bij belangrijke IT-beveiligingsincidenten treedt het directoraat-generaal Informatica op als contactpunt voor het beheer van de crisissituatie, door middel van coördinatie van de crisisteams voor IT-beveiligingsincidenten.

13. In noodsituaties kan de directeur-generaal van het directoraat-generaal Informatica beslissen een noodprocedure voor IT-beveiliging in te leiden. Het directoraat-generaal Informatica ontwikkelt noodprocedures en legt deze ter goedkeuring voor aan de ISSB.

14. Het directoraat-generaal Informatica brengt aan de ISSB en aan de hoofden van de getroffen afdelingen van de Commissie verslag uit over de uitvoering van de noodprocedures.

De processen die met deze verantwoordelijkheden en activiteiten samenhangen, worden in uitvoeringsbepalingen nader uitgewerkt.

HOOFDSTUK 4

SLOTBEPALINGEN

Artikel 16

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 17

Verband met andere handelingen

De bepalingen van dit besluit laten Besluit (EU, Euratom) 2015/443, Besluit (EU, Euratom) 2015/444, Verordening (EG) nr. 45/2001, Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad ([1]), Besluit 2002/47/EG, EGKS, Euratom van de Commissie ([2]), Verordening (EU, Euratom) nr. 883/2013 van het Europees Parlement en de Raad ([3]) en Besluit 1999/352/EG, EGKS, Euratom onverlet.

Artikel 18

Intrekking en overgangsmaatregelen

Besluit C(2006) 3602 van 16 augustus 2006 wordt ingetrokken.

De uitvoeringsbepalingen en IT-beveiligingsnormen die uit hoofde van artikel 10 van Besluit C(2006) 3602 zijn vastgesteld, blijven, voor zover zij niet strijdig zijn met onderhavig besluit, van kracht totdat zij worden vervangen door de uit hoofde van artikel 13 van onderhavig besluit vast te stellen uitvoeringsbepalingen en normen. Verwijzingen naar artikel 10 van Besluit C(2006) 3602 worden gelezen als verwijzingen naar artikel 13 van onderhavig besluit.

Artikel 19

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, 10 januari 2017.

Voor de Commissie
De voorzitter
Jean-Claude JUNCKER

([1]) Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie (PB L 145 van 31.5.2001, blz. 43).
([2]) Besluit 2002/47/EG, EGKS, Euratom van de Commissie van 23 januari 2002 tot wijziging van haar reglement van orde (PB L 21 van 24.1.2002, blz. 23).
([3]) Verordening (EU, Euratom) nr. 883/2013 van het Europees Parlement en de Raad van 11 september 2013 betreffende onderzoeken door het Europees Bureau voor fraudebestrijding (OLAF) en tot intrekking van Verordening (EG) nr. 1073/1999 van het Europees Parlement en de Raad en van Verordening (Euratom) nr. 1074/1999 (PB L 248 van 18.9.2013, blz. 1).