BESLUIT (EU) 2022/640 VAN DE COMMISSIE

van 7 april 2022

betreffende uitvoeringsvoorschriften inzake de rollen en verantwoordelijkheden van de belangrijkste veiligheidsactoren

DE EUROPESE COMMISSIE,

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

Gezien Besluit (EU, Euratom) 2015/443 van de Commissie van 13 maart 2015 betreffende veiligheid binnen de Commissie ([1]),

Gezien Besluit (EU, Euratom) 2015/444 van de Commissie van 13 maart 2015 betreffende de veiligheidsvoorschriften voor de bescherming van gerubriceerde EU-informatie ([2]),

Overwegende hetgeen volgt:

(1) De Besluiten (EU, Euratom) 2015/443 en (EU, Euratom) 2015/444 zijn van toepassing op alle afdelingen en gebouwen van de Commissie.

(2) Indien noodzakelijk moeten uitvoeringsbepalingen ter aanvulling of ondersteuning van Besluit (EU, Euratom) 2015/444 worden vastgesteld overeenkomstig artikel 60 van dat besluit.

(3) De beveiligingsmaatregelen om gerubriceerde EU-informatie ("EU classified information", EUCI) gedurende de gehele levenscyclus ervan te beschermen, moeten evenredig zijn met de beveiligingsrubricering van die informatie.

(4) De beveiligingsmaatregelen voor de bescherming van communicatie- en informatiesystemen binnen de Commissie zijn vastgelegd in Besluit (EU, Euratom) 2017/46 van de Commissie ([3]), en met name artikel 3 over de beginselen van IT-beveiliging binnen de Commissie, en artikel 9 over systeemeigenaars.

(5) Het doel van de uitvoeringsvoorschriften inzake de rollen en verantwoordelijkheden van de belangrijkste veiligheidsactoren is richtsnoeren te verstrekken inzake de voorwaarden en taken die voor die rollen zijn vastgesteld in de Besluiten (EU, Euratom) 2015/443 en (EU, Euratom) 2015/444.

(6) Artikel 36, lid 7, van Besluit (EU, Euratom) 2015/444 stelt een aantal extra veiligheidsgerelateerde rollen vast die door de veiligheidsautoriteit van de Commissie moeten worden vervuld. De taken in verband met deze rollen zijn vastgelegd in dit besluit.

(7) Overeenkomstig Besluit (EU, Euratom) 2015/444 hebben lokale veiligheidsagenten en controlefunctionarissen van het register specifieke verantwoordelijkheden voor de bescherming van gerubriceerde EU-informatie in hun afdelingen.

(8) Op 4 mei 2016 heeft de Commissie een besluit ([4]) vastgesteld waarbij het voor veiligheid bevoegde lid van de Commissie wordt gemachtigd om namens de Commissie en onder haar verantwoordelijkheid de in artikel 60 van Besluit (EU, Euratom) 2015/444 bedoelde uitvoeringsbepalingen vast te stellen; vervolgens heeft het voor veiligheid bevoegde lid van de Commissie op 13 april 2021 namens de Commissie en onder haar verantwoordelijkheid een besluit ([5]) vastgesteld waarbij deze uitvoeringsvoorschriften worden gesubdelegeerd aan de directeur-generaal van het directoraat-generaal Personele Middelen en Veiligheid,

([1]) PB L 72 van 17.3.2015, blz. 41.
([2]) PB L 72 van 17.3.2015, blz. 53.
([3]) Besluit (EU, Euratom) 2017/46 van de Commissie van 10 januari 2017 over de beveiliging van communicatie- en informatiesystemen binnen de Europese Commissie (PB L 6 van 11.1.2017, blz. 40).
([4]) Besluit C(2016) 2797 van 4 mei 2016 betreffende een machtiging inzake veiligheid.
([5]) Besluit C(2021) 2684 van 13 april 2021 tot verlening van een subdelegatie van bevoegdheden die zijn verleend bij Besluit C(2016) 2797 van de Commissie betreffende een machtiging inzake veiligheid.

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

HOOFDSTUK 1

Algemene bepalingen

Artikel 1

Onderwerp en toepassingsgebied

1. In dit besluit worden de rollen en verantwoordelijkheden vastgesteld van de belangrijkste veiligheidsactoren die krachtens Besluiten (EU, Euratom) 2015/443 en (EU, Euratom) 2015/444 verantwoordelijk zijn voor de bescherming van gerubriceerde EU-informatie (EUCI) bij de Commissie.

2. Dit besluit is van toepassing op alle afdelingen van de Commissie en in al haar gebouwen.

HOOFDSTUK 2

Directoraat-generaal Personele Middelen en Veiligheid

Artikel 2

Veiligheidsautoriteit van de Commissie

1. De directeur van het directoraat Veiligheid van het directoraat-generaal Personele Middelen en Veiligheid is de veiligheidsautoriteit van de Commissie ("Commission Security Authority", CSA) bedoeld in artikel 7 van Besluit (EU, Euratom) 2015/444.

2. De CSA vervult haar rollen op de volgende gebieden, zoals vastgesteld in Besluit (EU, Euratom) 2015/444, overeenkomstig de artikelen 3 tot en met 7 van dit besluit:

a) veiligheid van personeel;

b) fysieke beveiliging;

c) beheer van EUCI;

d) homologatie van communicatie- en informatiesystemen (CIS) voor de behandeling van EUCI;

e) industriële beveiliging, alsmede

f) uitwisseling van gerubriceerde informatie.

3. De CSA organiseert verplichte opleiding voor de lokale veiligheidsagenten (LSO's), de plaatsvervangende LSO's, de registercontrolefunctionarissen (RCO's) en de plaatsvervangende RCO's over hun verantwoordelijkheden en taken.

Artikel 3

Instantie voor informatieborging

De instantie voor informatieborging ("Information Assurance Authority", IAA) is verantwoordelijk voor de volgende activiteiten in verband met de bescherming van EUCI:

a) ontwikkelen van beveiligingsbeleid en beveiligingsrichtsnoeren voor informatieborging en monitoren van de doeltreffendheid en relevantie ervan;

b) beschermen en beheren van technische informatie over encryptieproducten;

c) ervoor zorgen dat de maatregelen voor informatieborging in overeenstemming zijn met het beveiligings- en aanbestedingsbeleid van de Commissie, voor zover van toepassing;

d) ervoor zorgen dat encryptieproducten worden geselecteerd overeenkomstig het beleid inzake de geschiktheid en selectie ervan;

e) overleggen met systeemeigenaars, systeemaanbieders, veiligheidsactoren en vertegenwoordigers van gebruikers met betrekking tot beveiligingsbeleid en beveiligingsrichtsnoeren voor informatieborging.

Artikel 4

Veiligheidshomologatieautoriteit

1. De CSA is verantwoordelijk voor de homologatie van beveiligde zones die voldoen aan de eisen van artikel 18 van Besluit (EU, Euratom) 2015/444 en van CIS waarmee EUCI wordt behandeld.

2. De afdelingen van de Commissie raadplegen de veiligheidshomologatieautoriteit ("Security Accreditation Authority", SAA) in overleg met hun LSO en hun LISO, naargelang het geval, wanneer een afdeling voornemens is:

a) een beveiligde zone aan te leggen;

b) een CIS voor de behandeling van EUCI in gebruik te nemen;

c) andere apparatuur te installeren voor de behandeling van gerubriceerde informatie, met inbegrip van verbindingen met de CIS van een derde partij.

De SAA verstrekt advies over deze activiteiten tijdens zowel het plannings- als het bouw- of ontwikkelingsproces.

3. EUCI wordt niet behandeld in een beveiligde zone of CIS voordat de veiligheidshomologatieautoriteit die omgeving op de passende rubriceringsgraad van EUCI heeft gehomologeerd.

4. De eisen voor de homologatie van een beveiligde zone omvatten:

a) goedkeuring van de plannen voor de beveiligde zone;

b) goedkeuring van alle contracten voor werkzaamheden die door externe contractanten worden uitgevoerd, rekening houdend met de bepalingen inzake industriële beveiliging, zoals de vereisten inzake veiligheidsverklaringen van de contractanten en hun personeel;

c) beschikbaarheid van alle vereiste verklaringen en certificaten van overeenstemming;

d) een fysieke inspectie van de beveiligde zone om na te gaan of de bouwmaterialen en -methoden, toegangscontroles, beveiligingsapparatuur en andere artikelen voldoen aan de eisen van de CSA;

e) validering van de maatregelen tegen elektromagnetische straling voor elke technisch beveiligde zone;

f) goedkeuring van de operationele beveiligingsprocedures (SecOP's) voor de beveiligde zone.

5. De eisen voor de goedkeuring van een CIS voor de behandeling van EUCI omvatten:

a) ontwikkeling van een strategie voor de homologatie van het systeem;

b) validering van het beveiligingsplan van het CIS, op basis van een risicobeheermethode;

c) validering van de SecOP's voor het CIS;

d) validering van alle andere vereiste veiligheidsdocumenten, zoals bepaald door de veiligheidshomologatieautoriteit;

e) goedkeuring van het gebruik van encryptietechnologieën;

f) validering van de maatregelen tegen elektromagnetische straling voor een CIS dat informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger behandelt;

g) een inspectie van het CIS om na te gaan of de gedocumenteerde beveiligingsmaatregelen correct worden uitgevoerd.

6. Wanneer aan de homologatievereisten is voldaan, geeft de veiligheidshomologatieautoriteit een formele machtiging af voor de behandeling van EUCI in de beveiligde zone of CIS, voor een bepaalde maximale rubriceringsgraad van EUCI en voor hoogstens vijf jaar, afhankelijk van het niveau van de behandelde EUCI en de daaraan verbonden risico's.

7. Bij kennisgeving van een inbreuk op de beveiliging of van een aanzienlijke verandering in de opzet of de beveiligingsmaatregelen van een beveiligde zone of CIS, beoordeelt de veiligheidshomologatieautoriteit de machtiging om EUCI te behandelen en trekt zij deze zo nodig in tot de vastgestelde problemen zijn verholpen.

Artikel 5

Tempest-instantie

1. Tempest-beveiligingsmaatregelen worden genomen ter bescherming van CIS's die informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger behandelen, en kunnen worden toegepast voor informatie met rubricering RESTREINT UE/EU RESTRICTED.

2. De Tempest-instantie ("TEMPEST Authority") wordt belast met de goedkeuring van maatregelen ter bescherming tegen compromittering van EUCI door onopzettelijke elektromagnetische emissies.

3. Op verzoek van een systeemeigenaar van een CIS dat EUCI behandelt, geeft de Tempest-instantie specificaties voor Tempest-beveiligingsmaatregelen die passend zijn voor de rubriceringsgraad van de informatie.

4. De TEMPEST-instantie voert technische tests uit tijdens de homologatie van beveiligde zones en CIS voor de behandeling van EUCI met rubriceringsgraad CONFIDENTIAL UE/EU CONFIDENTIAL of hoger en geeft, na succesvolle tests, een Tempest-certificaat af.

5. In een Tempest-certificaat wordt ten minste het volgende vermeld:

a) de testdatum;

b) een beschrijving van de Tempest-beveiligingsmaatregelen, met plattegronden van het pand;

c) de datum waarop het certificaat zijn geldigheid verliest;

d) wijzigingen die de certificering ongeldig maken;

e) de handtekening van de Tempest-instantie.

6. Een LSO of een organisator van vergaderingen die in overleg met de LSO een gerubriceerde vergadering moet organiseren, kan de Tempest-instantie verzoeken vergaderzalen te testen om ervoor te zorgen dat deze technisch beveiligd zijn.

Artikel 6

Instantie voor de goedkeuring van cryptografische producten (Crypto Approval Authority)

1. De instantie voor de goedkeuring van cryptografische producten is verantwoordelijk voor de goedkeuring van het gebruik van encryptietechnologieën.

2. De instantie voor de goedkeuring van cryptografische producten moet richtsnoeren verstrekken inzake de voorschriften voor het gebruik en de goedkeuring van encryptietechnologieën.

3. De instantie voor de goedkeuring van cryptografische producten keurt het gebruik van encryptieoplossingen goed op basis van een verzoek van de systeemeigenaar. Goedkeuring wordt verleend op basis van een bevredigende beoordeling van ten minste:

a) de beveiligingsnoodzaak van de te beschermen informatie;

b) een overzicht van de CIS die bij de oplossing betrokken zijn;

c) een beoordeling van de inherente en restrisico's;

d) een beschrijving van de voorgestelde oplossing;

e) de SecOP's voor de encryptieoplossing.

4. De instantie voor de goedkeuring van cryptografische producten houdt een register bij van goedgekeurde encryptieoplossingen.

Artikel 7

Instantie voor de distributie van cryptografische producten

1. De instantie voor de distributie van cryptografische producten ("Crypto Distribution Authority") is verantwoordelijk voor de distributie van cryptografische producten voor de bescherming van EUCI (met name encryptieapparatuur, cryptografische sleutels, certificaten en aanverwante authenticatiemiddelen) aan:

a) gebruikers of afdelingen binnen de Commissie voor CIS die door externe partijen worden beheerd;

b) gebruikers of organisaties buiten de Commissie voor CIS die door de Commissie worden beheerd.

2. De instantie voor de distributie van cryptografische producten kan de distributie van cryptografisch materiaal voor derden aan andere afdelingen delegeren overeenkomstig artikel 17, lid 3, van Besluit (EU, Euratom) 2015/443.

3. De instantie voor de distributie van cryptografische producten zorgt ervoor dat al het cryptografisch materiaal wordt verzonden via beveiligde kanalen die bescherming bieden tegen en bewijs weergeven van manipulatie, overeenkomstig de beveiligingsvoorschriften die van toepassing zijn op de rubriceringsgraad van de met dat materiaal te beschermen EUCI.

4. De instantie voor de distributie van cryptografische producten verstrekt richtsnoeren aan de LSO en, in voorkomend geval, aan de plaatselijke informatiebeveiligingsfunctionaris van elke afdeling van de Commissie die betrokken is bij de productie, de distributie of het gebruik van het cryptografisch materiaal.

5. De instantie voor de distributie van cryptografische producten zorgt ervoor dat voor het distributieproces geschikte SecOP's worden vastgesteld.

HOOFDSTUK 3

Afdelingen van de Commissie

Artikel 8

Afdelingshoofden

1. Elk afdelingshoofd benoemt:

a) een LSO en, in voorkomend geval, een of meer plaatsvervangers voor de afdeling of het kabinet;

b) een RCO en, in voorkomend geval, een of meer plaatsvervangers voor elke afdeling die een EUCI-register beheert;

c) een systeemeigenaar voor elk CIS waarmee EUCI wordt behandeld.

2. Het afdelingshoofd vraagt de directeur van het directoraat Veiligheid van het directoraat-generaal Personele Middelen en Veiligheid om goedkeuring voordat de LSO's, plaatsvervangende LSO's, RCO's en plaatsvervangende RCO's worden benoemd.

3. Het afdelingshoofd stelt, in overleg met de LSO, vast voor welke functies een veiligheidsverklaring voor toegang tot EUCI vereist is. Kandidaten voor dergelijke functies worden er tijdens de aanwervingsprocedure van in kennis gesteld dat een veiligheidsverklaring is vereist.

4. Het hoofd van een afdeling die EUCI bewaart, is verantwoordelijk voor het activeren van noodplannen voor vernietiging en evacuatie, indien nodig. De plannen bevatten een alternatief voor situaties waarin geen contact kan worden opgenomen met het afdelingshoofd.

Artikel 9

Systeemeigenaars van CIS waarmee EUCI wordt behandeld

1. De systeemeigenaar neemt in het kader van een project voor de implementatie van een CIS voor de behandeling van EUCI zo spoedig mogelijk contact op met de veiligheidshomologatieautoriteit om de relevante beveiligingsnormen en -vereisten vast te stellen en het proces van veiligheidsaccreditatie te starten.

2. De systeemeigenaar waarborgt dat de beveiligingsmaatregelen voldoen aan de eisen van de veiligheidshomologatieautoriteit en dat het CIS geen EUCI behandelt voordat het is gehomologeerd.

3. De systeemeigenaar verzoekt de instantie voor de goedkeuring van cryptografische producten het gebruik van encryptietechnologieën goed te keuren. Systeemeigenaars mogen geen versleutelingstechnologieën in productiesystemen toepassen zonder voorafgaande goedkeuring.

4. De systeemeigenaar raadpleegt de LISO van de afdeling over kwesties in verband met de beveiliging van CIS's.

5. De systeemeigenaar evalueert ten minste eenmaal per jaar de beveiligingsmaatregelen die op een systeem worden toegepast, met inbegrip van het beveiligingsplan.

6. Wanneer zich in een CIS een beveiligingsincident voordoet waarbij wordt aangegeven dat het CIS EUCI niet langer passend kan beschermen, stelt de systeemeigenaar de LSO daarvan in kennis en neemt hij onmiddellijk contact op met de veiligheidshomologatieautoriteit voor advies over de te volgen aanpak. In dat geval kan de homologatie worden opgeschort en kan het systeem buiten werking worden gesteld totdat passende corrigerende maatregelen zijn genomen.

7. De systeemeigenaar verleent de veiligheidshomologatieautoriteit te allen tijde volledige steun bij het vervullen van de taken die deze instantie heeft met betrekking tot de homologatie van het CIS.

Artikel 10

Operationele instantie voor informatieborging

Het is de taak van de operationele instantie voor informatieborging om voor elk CIS:

a) beveiligingsdocumentatie op te stellen die in overeenstemming is met het beveiligingsbeleid en de beveiligingsrichtsnoeren, met name het beveiligingsplan, de aan het systeem gerelateerde SecOP's en de cryptografische documentatie in het kader van de homologatieprocedure van het CIS;

b) deel te nemen aan de selectie en het testen van de systeemspecifieke maatregelen, apparatuur en software voor de technische beveiliging, teneinde toezicht te houden op de implementatie ervan en ervoor te zorgen dat deze veilig worden geïnstalleerd, geconfigureerd en onderhouden overeenkomstig de beveiligingsdocumentatie;

c) deel te nemen aan de selectie van Tempest-beveiligingsmaatregelen en -apparatuur, indien vereist in het beveiligingsplan, en er in samenwerking met de Tempest-instantie voor te zorgen dat deze veilig worden geïnstalleerd en onderhouden;

d) toezicht te houden op de uitvoering en toepassing van de SecOP's die betrekking hebben op de werking van het systeem;

e) encryptieproducten te beheren en te gebruiken, in samenwerking met de instantie voor de distributie van cryptografische producten, teneinde de passende bewaring van cryptografisch materiaal en gecontroleerde producten te waarborgen en, zo nodig, voor de generatie van cryptografische variabelen te zorgen;

f) veiligheidsanalyses, -beoordelingen en -tests uit te voeren, in het bijzonder om risicorapporten op te stellen, zoals vereist door de veiligheidshomologatieautoriteit;

g) CIS-specifieke opleidingen over informatieborging aan te bieden;

h) CIS-specifieke beveiligingsmaatregelen te implementeren en toe te passen.

HOOFDSTUK 4

Lokale veiligheidsagent

Artikel 11

Benoeming van de LSO

1. De LSO en de plaatsvervangende LSO's zijn ambtenaren of tijdelijke functionarissen.

2. Alle LSO's en plaatsvervangende LSO's beschikken over een geldige veiligheidsmachtiging voor toegang tot EUCI tot rubriceringsgraad SECRET UE/EU SECRET en, indien nodig, tot rubriceringsgraad TRES SECRET UE/EU TOP SECRET. De LSO of plaatsvervangende LSO verkrijgt de veiligheidsmachtiging voordat zij worden benoemd.

3. De vertegenwoordigingen van de Commissie kunnen de CSA verzoeken een uitzondering toe te staan op de vereisten van de leden 1 en 2.

Artikel 12

Operationele beveiligingsprocedures voor beveiligde zones

1. De LSO van de betrokken afdeling van de Commissie stelt SecOP's op voor elke beveiligde zone die onder zijn verantwoordelijkheid valt.

2. De LSO zorgt ervoor dat de SecOP's de volgende vereisten bevatten:

a) alleen personeelsleden met een geldige veiligheidsmachtiging en een bewezen noodzaak om toegang te krijgen tot documenten met rubriceringsgraad CONFIDENTIEL UE/EU CONFIDENTIAL of hoger krijgen onbegeleide toegang tot een beveiligde zone tijdens kantooruren;

b) onbegeleide toegang tot een beveiligde zone wordt buiten kantooruren alleen verleend aan de LSO van de afdeling, de RCO("s) van de beveiligde zone, hun plaatsvervangers en gemachtigd personeel van het directoraat Veiligheid van het directoraat-generaal Personele Middelen en Veiligheid;

c) opname- en communicatieapparatuur, zoals mobiele telefoons, computers, camera's of andere slimme apparaten, is niet toegestaan in beveiligde zones zonder voorafgaande toestemming van de CSA; elke uitzondering moet vooraf bij de bevoegde toezichthoudende autoriteit worden aangevraagd; de LSO fungeert als contactpunt;

d) al het interne of externe personeel dat toegang tot een beveiligde zone nodig heeft, maar niet aan de criteria van punt a) voldoet, wordt te allen tijde begeleid door een naar behoren gemachtigd, toezichthoudend personeelslid; in voorkomend geval wordt elke toegang tot een beveiligde zone geregistreerd in een logboek dat bij de ingang van de beveiligde zone wordt bijgehouden;

e) de LSO zorgt ervoor dat de inbraakdetectiesystemen voor het toezicht op een beveiligde zone te allen tijde actief zijn en naar behoren functioneren, en beheert alle bijbehorende wachtwoorden, sleutels, PIN's en andere toegangs- en authenticatiemechanismen;

f) alarmsignalen in een beveiligde zone worden gemeld aan het directoraat Veiligheid van het directoraat-generaal Personele Middelen en Veiligheid, dat de LSO daarvan onmiddellijk in kennis stelt;

g) de LSO van de afdeling waar zich de beveiligde zone bevindt, houdt een register bij van elke interventie naar aanleiding van een alarmsignaal of een veiligheidsincident;

h) er worden procedures ingesteld voor het geval er een alarm afgaat of zich een andere noodsituatie voordoet binnen de beveiligde zone, onder meer voor het evacueren van het personeel en het waarborgen van een snelle reactie van een noodteam onder het gezag van de CSA en, indien nodig, externe nooddiensten;

i) de LSO meldt elke inbreuk op de beveiliging die plaatsvindt in of in verband met een beveiligde zone, onmiddellijk aan de CSA met het oog op het vaststellen van de passende reactie;

j) afzonderlijke kantoren, kamers en kluizen binnen een beveiligde zone worden afgesloten wanneer zij onbewaakt worden achtergelaten;

k) het personeel zorgt ervoor dat gerubriceerde informatie niet op de gang of in andere gemeenschappelijke zones van de beveiligde zone wordt besproken in de nabijheid van niet-gemachtigde personen.

Artikel 13

Beveiligingssleutels en -combinaties

1. De LSO heeft de algemene verantwoordelijkheid voor de correcte behandeling en opslag van sleutels en combinaties die worden gebruikt in of om toegang te krijgen tot beveiligde zones. Sleutels en combinaties worden opgeslagen in een beveiligd opbergmiddel en beschermd op ten minste hetzelfde rubriceringsgraad als het materiaal waartoe zij toegang geven.

2. De LSO houdt een register bij van beveiligde opbergmiddelen en kluizen, samen met een actuele lijst van alle personeelsleden die niet-begeleide toegang tot deze ruimten hebben.

3. De LSO houdt een register bij van sleutels voor beveiligde opbergmiddelen en kluizen, waarin ook wordt genoteerd aan welke personeelsleden deze zijn verstrekt. Voor elke afgegeven sleutel wordt een ontvangstbewijs bewaard, met vermelding van het identificatiekenmerk van de sleutel, de ontvanger, de datum en het tijdstip.

4. Sleutels en combinaties worden alleen afgegeven aan personeelsleden voor wie een "noodzaak tot kennisneming" geldt en aan wie de passende machtiging voor toegang tot EUCI is verleend. De LSO moet de betrokken sleutel terugnemen wanneer niet langer aan die voorwaarden wordt voldaan.

5. De LSO bewaart reservesleutels en een schriftelijk overzicht van elke codecombinatie in afzonderlijke verzegelde, ondoorzichtige, getekende en gedateerde enveloppen, die het voor de sleutels verantwoordelijke personeelslid ter beschikking moet stellen. Deze enveloppen worden bewaard in een beveiligd opbergmiddel waarvoor de hoogste rubriceringsgraad van het in de desbetreffende opbergmiddel of kluis opgeslagen materiaal geldt.

6. Indien bij een wijziging van combinatie of een sleutelrotatie een enveloppe sporen van manipulatie of beschadiging vertoont, behandelt de LSO dit als een veiligheidsincident en stelt hij de CSA daarvan onmiddellijk in kennis.

7. Wijzigingen van de codecombinatie van beveiligde opbergmiddelen in beveiligde zones worden uitgevoerd onder toezicht van de LSO. De combinaties worden ten minste om de twaalf maanden opnieuw ingesteld en telkens wanneer:

a) een nieuw opbergmiddel wordt ontvangen of een nieuw slot wordt aangebracht (met name moeten de standaardcombinaties onmiddellijk worden gewijzigd);

b) er wordt vermoed of duidelijk is dat compromittering heeft plaatsgevonden;

c) toegang niet langer is vereist voor een persoon die over een combinatie beschikt.

8. De LSO houdt een register bij van de data van de in lid 7 bedoelde veranderingen van de combinatie.

Artikel 14

Noodplannen voor evacuatie en vernietiging van EUCI

1. De LSO assisteert het afdelingshoofd bij het opstellen van noodplannen voor evacuatie en vernietiging van EUCI, op basis van richtsnoeren van HR.DS.

2. De LSO zorgt ervoor dat alle uitrusting die nodig is voor de uitvoering van de in lid 1 bedoelde plannen gemakkelijk beschikbaar is en goed wordt onderhouden.

3. De LSO evalueert, samen met de functionarissen die zijn aangewezen in de in lid 1 bedoelde plannen, ten minste om de twaalf maanden de adequaatheid van de plannen en neemt eventueel maatregelen om ze bij te werken.

Artikel 15

Veiligheidsmachtigingen

1. De LSO houdt een register bij van alle functies binnen de afdeling waarvoor een veiligheidsmachtiging van de Commissie vereist is en van het personeel dat deze functies vervult. Het vereiste van een veiligheidsmachtiging moet bij de aanwervingsprocedure in de kennisgeving van vacature worden vermeld en tijdens het sollicitatiegesprek aan de kandidaat worden meegedeeld.

2. De LSO houdt toezicht op alle verzoeken om veiligheidsmachtigingen voor toegang tot EUCI. De LSO is het contactpunt binnen de afdeling en onderhoudt contact met de CSA voor de veiligheidsmachtigingen.

3. De LSO initieert het verzoek om de veiligheidsmachtigingsprocedure voor het betrokken personeelslid in te leiden en zorgt ervoor dat het personeelslid de vragenlijst voor de nationale veiligheidsverklaring onverwijld terugstuurt naar de CSA.

4. De LSO zorgt ervoor dat de personeelsleden van de afdeling die over een veiligheidsverklaring beschikken, de verplichte EUCI-briefing volgen om hun veiligheidsmachtiging te verkrijgen.

5. De LSO onderhoudt regelmatig contact met de personeelsdienst van de afdeling om zich te laten informeren over alle personeelswisselingen met betrekking tot functies waarvoor een veiligheidsmachtiging vereist is, en stelt de CSA onmiddellijk in kennis van dergelijke wijzigingen.

6. De LSO stelt de CSA in kennis van de aankomst van een nieuw personeelslid dat over een veiligheidsverklaring beschikt en een functie aanvaardt waarvoor een veiligheidsmachtiging vereist is.

7. De LSO zorgt ervoor dat de personeelsleden van de afdeling de procedure voor de verlenging van een veiligheidsverklaring binnen de vereiste termijn afronden. Elk personeelslid dat weigert de procedure te voltooien, is verplicht over te gaan naar een functie waarvoor geen veiligheidsmachtiging nodig is.

Artikel 16

EUCI-register

1. Wanneer een afdeling een EUCI-register beheert, houdt de LSO toezicht op de activiteiten van de RCO's met betrekking tot de behandeling van EUCI en de naleving van de beveiligingsvoorschriften inzake de bescherming van EUCI.

2. De LSO voert ten minste om de twaalf maanden en bij een wissel van een RCO of plaatsvervangend RCO de volgende controles uit:

a) een steekproefsgewijze controle van documenten in het EUCI-register om de status daarvan en de correctheid van het register van gerubriceerde documenten te bevestigen;

b) een steekproefsgewijze controle van bewijzen van ontvangst en toezending met betrekking tot de distributie van EUCI vanuit en naar het EUCI-register;

c) een steekproefsgewijze controle van vernietigingscertificaten.

3. Ten minste eenmaal per maand verricht de LSO steekproefsgewijze controles met betrekking tot het register van gerubriceerde documenten en met betrekking tot recentelijk ontvangen gerubriceerde documenten, om te waarborgen dat documenten correct worden geregistreerd.

4. Alle controles worden geregistreerd in het logboek van het register van gerubriceerde documenten.

Artikel 17

Overige verantwoordelijkheden op het gebied van beveiliging

De overige verantwoordelijkheden op het gebied van beveiliging van de LSO worden vastgesteld in een veiligheidsmededeling die met name betrekking heeft op de fysieke beveiliging van personen, panden en andere goederen, en op informatie.

HOOFDSTUK 5

Functionaris voor de registercontrole

Artikel 18

Benoeming van de RCO

1. De RCO en de plaatsvervangende RCO's zijn ambtenaren of tijdelijke functionarissen.

2. Alle RCO's en plaatsvervangende RCO's beschikken over een geldige veiligheidsmachtiging voor toegang tot EUCI tot rubriceringsgraad SECRET UE/EU SECRET en, indien nodig, tot rubriceringsgraad TRES SECRET UE/EU TOP SECRET. De RCO of plaatsvervangende RCO's verkrijgen de veiligheidsmachtiging voordat zij worden benoemd.

3. De vertegenwoordigingen van de Commissie kunnen de CSA verzoeken een uitzondering toe te staan op de vereisten van de leden 1 en 2.

Artikel 19

Verantwoordelijkheden

1. De RCO's registreren informatie die voor beveiligingsdoeleinden als CONFIDENTIEL UE/EU CONFIDENTIAL of hoger is gerubriceerd, bij:

a) aankomst in of vertrek uit een afdeling van de Commissie, of

b) aankomst in of vertrek uit een CIS.

2. De RCO's registreren alle gebeurtenissen in de levenscyclus van alle als CONFIDENTIEL UE/EU CONFIDENTIAL of hoger gerubriceerde informatie. De RCO's zorgen er ook voor dat een register wordt bijgehouden van alle informatie die als RESTREINT UE/EU RESTRICTED of op een gelijkwaardig niveau is gerubriceerd en die met derde landen en internationale organisaties wordt uitgewisseld. Dit wordt afgestemd met het door het secretariaat-generaal beheerde EUCI-register.

3. De RCO registreert documenten met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger in het register van gerubriceerde documenten en zorgt ervoor dat zij veilig in het EUCI-register worden opgeslagen.

4. De RCO assisteert het personeel van de Commissie bij het opstellen en verzenden van informatie met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger.

5. Wanneer documenten met rubricering CONFIDENTIEL UE/EU CONFIDENTIAL of hoger worden ontvangen van andere afdelingen of externe partijen, zorgt de RCO ervoor dat het afgiftebewijs aan de auteur wordt teruggezonden.

6. Voordat de RCO een personeelslid toestemming verleent voor toegang tot een gerubriceerd document in het EUCI-register, verifieert de RCO bij de LSO dat het personeelslid houder is van een veiligheidsmachtiging van de CSA.

7. De RCO registreert alle personeelsleden die het EUCI-register betreden en verlaten, maar geen veiligheidsmachtiging hebben voor toegang zonder begeleiding, en begeleidt hen gedurende het bezoek.

8. Wanneer een personeelslid een document voor raadpleging meeneemt uit het EUCI-register, waarborgt de RCO dat diegene op de hoogte is van de relevante compenserende veiligheidsmaatregelen en het document terugbrengt zodra hij het niet meer nodig heeft. De RCO waarschuwt het personeel dat een dergelijk document zo spoedig mogelijk moet worden teruggebracht.

9. Het EUCI-register geeft een koerierscertificaat af als gerubriceerde documenten worden meegenomen naar een ander land dan dat waar het register is gevestigd.

10. Nadere regels voor de registratie van gerubriceerde documenten door de RCO's worden vastgesteld in een veiligheidsmededeling.

Artikel 20

Verlaging van rubricering en derubricering

De RCO verleent de als auteur aangemerkte afdeling bijstand bij het beoordelen van geregistreerde EUCI om vast te stellen of de oorspronkelijke rubriceringsgraad nog passend is of kan worden verlaagd, dan wel of het document kan worden gederubriceerd.

Artikel 21

Vernietiging

1. RCO's zijn verantwoordelijk voor het vernietigen van als CONFIDENTIEL UE/EU CONFIDENTIAL en hoger gerubriceerde informatie, met goedgekeurde middelen en zo nodig in aanwezigheid van getuigen met een veiligheidsverklaring.

2. RCO's registreren elke vernietiging van als CONFIDENTIEL UE/EU CONFIDENTIAL of hoger gerubriceerde informatie in het register van gerubriceerde documenten en bewaren de betrokken vernietigingscertificaten in het EUCI-register.

Artikel 22

Aanvullende taken

1. De RCO verleent de LSO alle nodige bijstand bij het verrichten van toezichtswerkzaamheden in het EUCI-register.

2. De RCO meldt vermoedelijke of feitelijke beveiligingsincidenten aan de LSO, die deze weer meldt aan de CSA.

3. De RCO van het EUCI-register van een afdeling van de Commissie die een als CONFIDENTIEL UE/EU CONFIDENTIAL of hoger gerubriceerde vergadering organiseert, stelt de EUCI op die tijdens die vergadering zal worden behandeld en maakt afspraken met de organisator van de vergadering om te waarborgen dat alle documenten en afgiftebewijzen volgens de desbetreffende regels worden behandeld.

HOOFDSTUK 6

Slotbepalingen

Artikel 23

Transparantie

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

Artikel 24

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

Gedaan te Brussel, 7 april 2022.

Voor de Commissie,
namens de voorzitter,
Gertrud INGESTAD
Directeur-generaal
Directoraat-generaal Personele Middelen en Veiligheid