II

*(Mededelingen)*

# MEDEDELINGEN VAN DE INSTELLINGEN, ORGANEN EN INSTANTIES VAN DE EUROPESE UNIE

# EUROPEES PARLEMENT

## BESLUIT VAN HET BUREAU VAN HET EUROPEES PARLEMENT

**van 15 april 2013**

**over de regels voor de behandeling van vertrouwelijke informatie door het Europees Parlement**

(2014/C 96/01)

HET BUREAU VAN HET EUROPEES PARLEMENT,

Gelet op artikel 23, lid 12, van het Reglement van het Europees Parlement,

Overwegende hetgeen volgt:

(1) In het licht van het Kaderakkoord over de betrekkingen tussen het Europees Parlement en de Europese Commissie ([1]), dat op 20 oktober 2010 werd ondertekend („het Kaderakkoord"), en van het Interinstitutioneel Akkoord tussen het Europees Parlement en de Raad over het doorzenden aan en verwerken door het Europees Parlement van gerubriceerde informatie waarover de Raad beschikt met betrekking tot aangelegenheden die niet vallen onder het gemeenschappelijk buitenlands en veiligheidsbeleid ([2]), dat op 12 maart 2014 werd ondertekend („het Interinstitutioneel Akkoord"), is het nodig specifieke regels vast te stellen voor de behandeling van vertrouwelijke documenten door het Europees Parlement.

(2) Het Verdrag van Lissabon kent het Europees Parlement nieuwe taken toe en om de activiteiten van het Parlement te ontwikkelen op die gebieden die een bepaalde mate aan vertrouwelijkheid vereisen, is het nodig om basisbeginselen, minimumnormen inzake beveiliging en passende procedures vast te stellen voor de behandeling door het Europees Parlement van vertrouwelijke, waaronder gerubriceerde, informatie.

(3) De regels die in dit besluit zijn vastgelegd, beogen normen voor beveiliging en compatibiliteit te garanderen die gelijkwaardig zijn aan de regels die zijn vastgesteld door andere instellingen, organen en instanties die krachtens of op basis van de Verdragen zijn opgericht, of door de lidstaten, teneinde te komen tot een soepele werking van het besluitvormingsproces van de Europese Unie.

(4) De voorschriften van dit besluit laten de huidige en toekomstige regels inzake de toegang tot documenten onverlet die overeenkomstig artikel 15 van het Verdrag betreffende de werking van de Europese Unie (VWEU) zijn vastgesteld.

([1]) PB L 304 van 20.11.2010, blz. 47.
([2]) PB C 95 van 1.4.2014, blz. 1.

(5) De voorschriften van dit besluit laten de huidige en toekomstige regels inzake de bescherming van persoonsgegevens onverlet die overeenkomstig artikel 16 VWEU zijn vastgesteld.

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

*Artikel 1*

**Doelstelling**

Dit besluit regelt het beheer en de verwerking van vertrouwelijke informatie door het Europees Parlement, daaronder begrepen het genereren, het ontvangen, het verstrekken en het opslaan van vertrouwelijke informatie, met het oog op een passende bescherming van het vertrouwelijke karakter daarvan. Het geeft in het bijzonder uitvoering aan het Interinstitutioneel Akkoord en aan het Kaderakkoord, en met name bijlage II ervan..

*Artikel 2*

**Definities**

Voor de toepassing van dit besluit wordt verstaan onder:

a) „informatie": elke schriftelijke of mondelinge informatie, ongeacht de drager of de auteur;

b) „vertrouwelijke informatie": „gerubriceerde informatie"en niet-gerubriceerde „andere vertrouwelijke informatie";

c) „gerubriceerde informatie": „gerubriceerde EU-informatie" en „gelijkwaardige gerubriceerde informatie";

d) „gerubriceerde EU-informatie" (EUCI): informatie en materiaal, gerubriceerd als „TRÈS SECRET UE/ EU TOP SECRET", „SECRET UE/EU SECRET", „CONFIDENTIEL UE/EU CONFIDENTIAL" of „RESTREINT UE/EU RESTRICTED", waarvan openbaarmaking zonder machtiging de belangen van de Unie of van één of meer van haar lidstaten in meerdere of mindere mate zou kunnen schaden, ongeacht of dergelijke informatie afkomstig is van de instellingen, organen en instanties die krachtens of op basis van de Verdragen zijn opgericht. In dit verband is informatie en materiaal gerubriceerd als:

— „TRÈS SECRET UE/EU TOP SECRET" informatie en materiaal waarvan de openbaarmaking zonder machtiging in uitzonderlijke mate nadelig zou kunnen zijn voor de wezenlijke belangen van de Unie of van één of meer van haar lidstaten;

— „SECRET UE/EU SECRET" informatie en materiaal waarvan de openbaarmaking zonder machtiging in ernstige mate nadelig zou kunnen zijn voor de wezenlijke belangen van de Europese Unie of van één of meer van haar lidstaten;

— „CONFIDENTIEL UE/EU CONFIDENTIAL" informatie en materiaal waarvan de openbaarmaking zonder machtiging nadelige gevolgen zou kunnen hebben voor de wezenlijke belangen van de Europese Unie of van één of meer van haar lidstaten;

— „RESTREINT UE/EU RESTRICTED" informatie en materiaal waarvan de openbaarmaking zonder machtiging nadelig zou kunnen zijn voor de belangen van de Europese Unie of van één of meer van haar lidstaten;

e) „gelijkwaardige gerubriceerde informatie": gerubriceerde informatie die afkomstig is van de lidstaten, derde staten of internationale organisaties, voorzien is van een rubriceringsmarkering die gelijkwaardig is aan een van de voor EUCI gebruikte rubriceringsmarkeringen en door de Raad of de Commissie aan het Europees Parlement is toegezonden;

f) „andere vertrouwelijke informatie": andere niet-gerubriceerde vertrouwelijke informatie, met inbegrip van informatie waarop gegevensbeschermingsregels van toepassing zijn of die onder het beroepsgeheim valt, die binnen het Europees Parlement is gegenereerd of die door andere instellingen, organen en instanties die krachtens of op basis van de Verdragen zijn opgericht, of door de lidstaten aan het Europees Parlement is toegezonden;

g) „document": opgeslagen informatie, ongeacht de fysieke vorm of de kenmerken daarvan;

h) „materiaal": documenten, of machines of uitrustingen die zijn of worden vervaardigd;

i) „need to know": de noodzaak voor een persoon toegang te hebben tot vertrouwelijke informatie om een officiële functie of taak te kunnen vervullen;

j) „machtiging": een besluit, vastgesteld door de Voorzitter in het geval van leden van het Europees Parlement of door de secretaris-generaal in het geval van ambtenaren van het Europees Parlement en andere parlementaire medewerkers die in dienst van een fractie zijn, om een persoon tot op een bepaald niveau toegang tot gerubriceerde informatie te geven, op basis van een positief resultaat van een veiligheidsonderzoek (doorlichting) dat door een nationale autoriteit overeenkomstig nationale rechtsvoorschriften en in overeenstemming met de bepalingen van bijlage I, deel 2, is uitgevoerd;

k) „lager rubriceren" (downgrading): het verlagen van het niveau van rubricering;

l) „derubricering" (declassification): het opheffen van een rubricering;

m) „markering": een op „andere vertrouwelijke informatie" aangebracht teken ter aanduiding van vooraf vastgestelde specifieke instructies inzake de verwerking van die informatie of het terrein waarop een bepaald document betrekking heeft. Een markering kan ook worden aangebracht op gerubriceerde informatie teneinde bijkomende eisen aan de verwerking van die informatie te stellen;

n) „demarkering": het verwijderen van een markering;

o) „opsteller": de gemachtigde auteur van vertrouwelijke informatie;

p) „veiligheidsmededelingen": de in bijlage II vermelde uitvoeringsmaatregelen;

q) „instructies voor behandeling": technische instructies aan de diensten van het Europees Parlement inzake de omgang met vertrouwelijke informatie.

*Artikel 3*

**Basisbeginselen en minimumnormen**

1. De behandeling van vertrouwelijke informatie door het Europees Parlement vindt plaats volgens de basisbeginselen en minimumnormen vermeld in bijlage I, deel 1.

2. Het Europees Parlement zet in overeenstemming met die basisbeginselen en minimumnormen een beheerssysteem voor informatieveiligheid (Information Security Management System, ISMS) op**.** Het ISMS bestaat uit de veiligheidsmededelingen, de instructies voor behandeling en de relevante bepalingen van het Reglement. Het ISMS is gericht op het ondersteunen van het parlementaire en administratieve werk, terwijl het tegelijkertijd de bescherming van door het Europees Parlement behandelde vertrouwelijke informatie waarborgt, met volledige inachtneming van de regels die door de opsteller van de bewuste informatie zijn vastgesteld zoals opgenomen in de veiligheidsmededelingen.

De verwerking van vertrouwelijke informatie door middel van geautomatiseerde communicatie- en informatiesystemen (CIS) van het Europees Parlement vindt plaats in overeenstemming met het concept informatiezekerheid (IA) zoals bedoeld in veiligheidsmededeling 3.

3. De leden van het Europees Parlement kunnen informatie die tot en met het niveau „RESTREINT UE/EU RESTRICTED" is gerubriceerd zonder veiligheidsmachtiging raadplegen.

4. Wanneer de informatie in kwestie is gerubriceerd als „CONFIDENTIEL UE/EU CONFIDENTIAL" of op een gelijkwaardig niveau, wordt toegang ertoe verleend aan leden van het Europees Parlement die door de Voorzitter zijn gemachtigd overeenkomstig lid 5 of na ondertekening van een plechtige verklaring dat zij de inhoud van die informatie niet aan derden bekend zullen maken, de verplichting tot bescherming van als „CONFIDENTIEL UE/EU CONFIDENTIAL" gerubriceerde informatie zullen nakomen en zich bewust zijn van de gevolgen bij nalatigheid.

5. Wanneer de informatie in kwestie is gerubriceerd als „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau, wordt toegang verleend aan leden van het Europees Parlement die door de Voorzitter zijn gemachtigd nadat:

a) zij een veiligheidsonderzoek overeenkomstig bijlage I, deel 2, van dit besluit hebben ondergaan, of

b) een kennisgeving van een nationale bevoegde autoriteit is ontvangen dat de betrokken leden uit hoofde van hun functies overeenkomstig het nationaal recht naar behoren zijn gemachtigd.

6. Voordat hun toegang tot gerubriceerde informatie wordt verleend, worden de leden van het Europees Parlement geïnstrueerd over en bevestigen zij hun verantwoordelijkheden met betrekking tot de bescherming van die informatie overeenkomstig bijlage I. Tevens worden zij geïnstrueerd over de middelen waarmee die bescherming kan worden gewaarborgd.

7. De ambtenaren van het Europees Parlement en andere parlementaire medewerkers die in dienst van een fractie zijn, mogen vertrouwelijke informatie raadplegen indien zij een vastgestelde „need to know"-status hebben, en mogen vertrouwelijke informatie die boven het niveau „RESTREINT UE/EU RESTRICTED" is gerubriceerd raadplegen, indien zij over de passende veiligheidsmachtiging beschikken. De toegang tot gerubriceerde informatie wordt hun alleen verleend als zij zijn geïnstrueerd en schriftelijke instructies hebben ontvangen over hun verantwoordelijkheden met betrekking tot de bescherming van die informatie en de middelen waarmee die bescherming kan worden gewaarborgd, en als zij een verklaring hebben ondertekend waarin zij de ontvangst van die instructies bevestigen en zich tot naleving ervan overeenkomstig deze regels verplichten.

*Artikel 4*

**Het genereren van vertrouwelijke informatie en de administratieve behandeling daarvan door het Europees Parlement**

1. De Voorzitter van het Europees Parlement, de voorzitters van de betreffende parlementaire commissies en de secretaris-generaal en/of elk persoon die door hem schriftelijk is gemachtigd, mag vertrouwelijke informatie genereren en/of informatie rubriceren, zoals bepaald in de veiligheidsmededelingen.

2. Bij het genereren van gerubriceerde informatie, past de opsteller het passende niveau van rubricering toe in overeenstemming met de internationale normen en definities die in bijlage I zijn opgenomen. De opsteller bepaalt, als algemene regel, ook de geadresseerden die moeten worden gemachtigd om de informatie te raadplegen overeenkomstig het niveau van rubricering. Deze informatie wordt aan de afdeling Gerubriceerde gegevens (Classified Information Unit, CIU) meegedeeld op het moment dat de document bij de CIU wordt ingediend.

3. „Andere vertrouwelijke informatie" die onder het beroepsgeheim valt, wordt behandeld overeenkomstig de bijlagen I en II en de instructies voor behandeling.

*Artikel 5*

**Ontvangst van vertrouwelijke informatie door het Europees Parlement**

1. Vertrouwelijke informatie die door het Europees Parlement wordt ontvangen, wordt als volgt doorgegeven:

a) informatie die als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau is gerubriceerd, en „andere vertrouwelijke informatie": aan het secretariaat van het parlementaire orgaan dat/de parlementaire ambtsdrager die het verzoek daartoe heeft ingediend, of rechtstreeks aan de CIU;

b) informatie die als „CONFIDENTIEL UE/CONFIDENTIEL EU", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd: aan de CIU.

2. De registratie, opslag en traceerbaarheid van vertrouwelijke informatie worden, naargelang van het geval, hetzij door het secretariaat van het parlementaire orgaan dat/de parlementaire ambtsdrager die de informatie heeft ontvangen, hetzij door de CIU verzekerd.

3. In het geval van vertrouwelijke informatie die door de Commissie op grond van bijlage 2, punt 3.2, bij het Kaderakkoord wordt verstrekt, of in het geval van gerubriceerde informatie die door de Raad op grond van artikel 5, lid 4, van het Interinstitutioneel Akkoord wordt doorgezonden, worden de overeengekomen regelingen, die in onderlinge overeenstemming moeten worden vastgesteld met het oog op het waarborgen van de vertrouwelijkheid van de informatie, samen met de vertrouwelijke informatie gedeponeerd bij het secretariaat van het parlementaire orgaan/de parlementaire ambtsdrager of bij de CIU, naargelang van het geval.

4. De regelingen als bedoeld in lid 3 kunnen mutatis mutandis worden toegepast in het geval van vertrouwelijke informatie die door andere instellingen, organen en instanties die krachtens of op basis van de Verdragen zijn opgericht, of door de lidstaten wordt verstrekt.

5. Teneinde een beschermingsniveau te waarborgen dat in overeenstemming is met het rubriceringsniveau „TRÈS SECRET UE/EU TOP SECRET" of een gelijkwaardig niveau, richt de Conferentie van voorzitters een comité van toezicht op. Informatie die als „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd, wordt aan het Europees Parlement toegezonden in overeenstemming met nadere regelingen die moeten worden overeengekomen tussen het Europees Parlement en de instelling van de Unie die de informatie verstrekt.

*Artikel 6*

**Verstrekking van gerubriceerde informatie door het Europees Parlement aan derden**

Het Europees Parlement mag, indien, naargelang van het geval, de opsteller of de instelling van de Unie die de gerubriceerde informatie aan het Europees Parlement heeft toegezonden, daarmee vooraf schriftelijk heeft ingestemd, die gerubriceerde informatie aan derden verstrekken, op voorwaarde dat zij waarborgen dat bij de verwerking van die informatie, binnen hun diensten en gebouwen regels in acht worden genomen die gelijkwaardig zijn aan de regels die in dit besluit zijn vastgelegd.

*Artikel 7*

**Beveiligde ruimten**

1. Ten behoeve van het beheer van vertrouwelijke informatie richt het Europees Parlement een beveiligde zone en beveiligde leeszalen in.

2. De beveiligde zone biedt faciliteiten voor de registratie, raadpleging, archivering, verzending en verwerking van gerubriceerde informatie. Deze zone omvat onder meer een leeszaal en een vergaderzaal voor de raadpleging van gerubriceerde informatie en wordt beheerd door de CIU.

3. Buiten de beveiligde zone kunnen beveiligde leeszalen worden ingericht waar informatie die als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau gerubriceerd is, en „andere vertrouwelijke informatie" kan worden geraadpleegd. Die beveiligde leeszalen worden beheerd door de bevoegde diensten van het secretariaat van het parlementaire orgaan/de parlementaire ambtsdrager of door de CIU, naargelang van het geval. Zij bevatten geen fotokopieerapparatuur, telefoons, faxapparaten, scanners of andere technische middelen voor het vermenigvuldigen of het verzenden van documenten.

*Artikel 8*

**Registratie, verwerking en opslag van vertrouwelijke informatie**

1. Informatie die als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau is gerubriceerd, en „andere vertrouwelijke informatie" wordt geregistreerd en opgeslagen door de bevoegde diensten van het secretariaat van het parlementaire orgaan/de parlementaire ambtsdrager of door de CIU, al naar gelang wie de informatie heeft ontvangen.

2. Voor de verwerking van informatie die als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau is gerubriceerd, en „andere vertrouwelijke informatie" gelden de volgende voorwaarden:

a) de documenten worden persoonlijk aan het hoofd van het secretariaat overhandigd, die de documenten registreert en een bewijs van ontvangst verstrekt;

b) dergelijke documenten worden, wanneer ze niet worden gebruikt, op een afgesloten plaats bewaard, onder de verantwoordelijkheid van het secretariaat;

c) in geen geval mag de informatie op een andere drager worden opgeslagen of aan iemand worden doorgezonden. Dergelijke documenten kunnen worden vermenigvuldigd met behulp van naar behoren gehomologeerde apparatuur, zoals omschreven in de veiligheidsmededelingen;

d) de toegang tot bedoelde informatie is beperkt tot de personen die volgens de regelingen als bedoeld in artikel 4, lid 2, respectievelijk artikel 5, leden 3, 4 en 5, zijn aangewezen door de opsteller of de instelling van de Unie die de informatie aan het Europees Parlement heeft toegezonden;

e) het secretariaat van het parlementaire orgaan/de parlementaire ambtdrager houdt een lijst bij van de personen die de informatie hebben geraadpleegd, inclusief datum en tijdstip van raadpleging en zendt de lijst aan de CIU toe op het moment waarop de informatie bij de CIU wordt gedeponeerd.

3. Informatie die als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd, wordt door de CIU in de beveiligde zone geregistreerd, verwerkt en opgeslagen, overeenkomstig het specifieke rubriceringsniveau en zoals bepaald in de veiligheidsmededelingen.

4. In geval van overtreding van regels van de leden 1 tot en met 3, stelt de verantwoordelijke ambtenaar van het secretariaat van het parlementaire orgaan/de parlementaire ambtdrager of van de CIU, naargelang van het geval, de secretaris-generaal op de hoogte, die de zaak naar de Voorzitter doorverwijst indien het om een lid van het Europees Parlement gaat.

*Artikel 9*

**Toegang tot beveiligde ruimten**

1. Alleen de onderstaande personen hebben toegang tot de beveiligde zone:

a) personen die uit hoofde van artikel 3, leden 4 tot en met 7, de daar bewaarde informatie mogen raadplegen en die een aanvraag uit hoofde van artikel 10, lid 1, hebben ingediend;

b) personen die uit hoofde van artikel 4, lid 1, gemachtigd zijn om gerubriceerde informatie te genereren en die een aanvraag uit hoofde van artikel 10, lid 1, hebben ingediend;

c) de bij de CIU werkzame ambtenaren van het Europees Parlement;

d) de ambtenaren van het Europees Parlement die met het beheer van de CIS zijn belast;

e) wanneer nodig, de ambtenaren van het Europees Parlement die met veiligheid en brandveiligheid zijn belast;

f) schoonmaakpersoneel alleen in aanwezigheid van en onder strikt toezicht van een ambtenaar van de CIU.

2. De CIU kan elke onbevoegde persoon de toegang tot de beveiligde zone ontzeggen. Tegen een dergelijke toegangsweigering kan bezwaar worden aangetekend bij de Voorzitter, indien het verzoek om toegang door een lid van het Europees Parlement is gedaan, en bij de secretaris-generaal in alle andere gevallen.

3. De secretaris-generaal kan toestemming verlenen voor een vergadering van een beperkt aantal personen in de vergaderzaal gelegen in de beveiligde zone.

4. Alleen de onderstaande personen hebben toegang tot een beveiligde leeskamer:

a) de leden van het Europees Parlement, ambtenaren van het Europees Parlement en andere parlementaire medewerkers die in dienst van een fractie zijn, mits zij naar behoren zijn geïdentificeerd met het oog op het raadplegen of genereren van gerubriceerde informatie;

b) de ambtenaren van het Europees Parlement die met het beheer van de CIS zijn belast, ambtenaren van het secretariaat van het parlementaire orgaan/de parlementaire ambtdrager die de informatie hebben ontvangen, en ambtenaren van de CIU;

c) wanneer nodig, de ambtenaren van het Europees Parlement die met veiligheid en brandveiligheid zijn belast;

d) schoonmaakpersoneel alleen in aanwezigheid van en onder strikt toezicht van een ambtenaar die op het secretariaat van het parlementaire orgaan/de parlementaire ambtdrager c.q. in de CIU werkt.

5. Het bevoegde secretariaat van het parlementaire orgaan/de parlementaire ambtdrager c.q. de CIU kan elke onbevoegde persoon de toegang tot een beveiligde leeskamer ontzeggen. Tegen een dergelijke toegangsweigering kan bezwaar worden aangetekend bij de Voorzitter, indien het verzoek om toegang door een lid van het Europees Parlement is gedaan, en bij de secretaris-generaal in alle andere gevallen.

*Artikel 10*

**Raadplegen of genereren van vertrouwelijke informatie in beveiligde ruimten**

1. Een persoon die vertrouwelijke informatie in de beveiligde zone wenst te raadplegen of te genereren, deelt zijn naam van tevoren aan de CIU mee. De CIU controleert de identiteit van die persoon, en gaat na of de hij overeenkomstig de regelingen als bedoeld in artikel 3, leden 3 tot en met 7, artikel 4, lid 1, of artikel 5, leden 3, 4 en 5, gemachtigd is de vertrouwelijke informatie te raadplegen of te genereren.

2. Een persoon die overeenkomstig artikel 3, leden 3 en 7, vertrouwelijke informatie die als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau is gerubriceerd, of „andere vertrouwelijke informatie" in een beveiligde leeskamer wenst te raadplegen, deelt zijn of haar naam van tevoren aan de bevoegde diensten van het secretariaat van het parlementaire orgaan/de parlementaire ambtdrager of de CIU mee.

3. Behoudens in uitzonderlijke omstandigheden (bijv. wanneer in een kort tijdsbestek een groot aantal aanvragen voor raadpleging is ingediend) wordt telkens slechts één persoon tot een beveiligde ruimte toegelaten om vertrouwelijke informatie te raadplegen, zulks in aanwezigheid van een ambtenaar van het secretariaat van het parlementaire orgaan/de parlementaire ambtdrager of van de CIU.

4. Tijdens het proces van raadpleging zijn contact met de buitenwereld (ook per telefoon of met behulp van andere technische hulpmiddelen), het maken van aantekeningen en het fotokopiëren of fotograferen van de geraadpleegde vertrouwelijke gegevens verboden.

5. Alvorens een persoon toestemming te geven de beveiligde ruimte te verlaten, gaat de ambtenaar van het secretariaat van het parlementaire orgaan/de parlementaire ambtdrager of van de CIU na of de geraadpleegde vertrouwelijke informatie aanwezig, onaangetast en volledig is.

6. In geval van overtreding van bovenstaande regels stelt de ambtenaar van het secretariaat van het parlementaire orgaan/de parlementaire ambtdrager of van de CIU de secretaris-generaal op de hoogte, die de zaak naar de Voorzitter doorverwijst indien het om een lid van het Europees Parlement gaat.

*Artikel 11*

**Minimumnormen voor raadpleging van vertrouwelijke informatie in een vergadering achter gesloten deuren buiten de beveiligde ruimten**

1. Informatie die als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau is gerubriceerd, en „andere vertrouwelijke informatie" mag door leden van parlementaire commissies of andere politieke of bestuursorganen van het Europees Parlement in een vergadering achter gesloten deuren buiten de beveiligde ruimten worden geraadpleegd.

2. In de in lid 1 bedoelde omstandigheden draagt het voor de vergadering verantwoordelijke secretariaat van het parlementaire orgaan/de parlementaire ambtsdrager ervoor zorg dat de volgende voorwaarden in acht worden genomen:

a) alleen de personen die door de voorzitter van de bevoegde commissie/het bevoegde orgaan als deelnemers aan de vergadering zijn opgegeven, wordt toegestaan de vergaderzaal te betreden;

b) alle documenten zijn genummerd, worden aan het begin van de vergadering uitgedeeld en aan het eind weer ingezameld, en er mogen geen notities en geen fotokopieën of foto's van deze documenten worden gemaakt;

c) in de notulen van de vergadering wordt geen melding gemaakt van de inhoud van de discussie over de behandelde informatie. Slechts een eventueel genomen besluit mag in de notulen worden vermeld;

d) voor vertrouwelijke informatie die mondeling aan ontvangers in het Europees Parlement wordt verstrekt geldt een niveau van bescherming gelijkwaardig aan dat voor vertrouwelijke informatie die in schriftelijke vorm wordt verstrekt;

e) in vergaderzalen worden geen extra documenten voorradig worden gehouden;

f) aan het begin van de vergadering wordt slechts het vereiste aantal exemplaren van documenten aan de deelnemers en tolken overhandigd;

g) de voorzitter licht aan het begin van de vergadering de rubricerings-/markeringsgraad van de documenten toe;

h) de deelnemers mogen geen documenten uit de vergaderzaal verwijderen;

i) alle exemplaren van de documenten worden aan het eind van de vergadering door het secretariaat van het parlementaire orgaan/de parlementaire ambtdrager ingezameld en geregistreerd; en

j) er worden geen elektronische communicatieapparatuur of andere elektronische apparatuur meegenomen naar de vergaderzaal waar de vertrouwelijke informatie in kwestie wordt geraadpleegd of besproken.

3. Wanneer overeenkomstig de uitzonderingsbepalingen in bijlage II, punt 3.2.2, bij het Kaderakkoord en artikel 6, lid 5, van het Interinstitutioneel Akkoord informatie die is gerubriceerd als „CONFIDENTIEL UE/EU CONFIDENTIAL" of op een gelijkwaardig niveau, wordt besproken in een vergadering achter gesloten deuren, draagt het voor de vergadering verantwoordelijke secretariaat van het parlementaire orgaan/de parlementaire ambtsdrager er naast de inachtneming van de voorwaarden in lid 2 zorg voor dat de personen die als deelnemers aan de vergadering zijn opgegeven, voldoen aan de in artikel 3, leden 4 en 7, gestelde eisen.

4. In het in lid 3 bedoelde geval verstrekt de CIU aan het voor de vergadering achter gesloten deuren verantwoordelijke secretariaat van het parlementaire orgaan/de parlementaire ambtsdrager het vereiste aantal exemplaren van de te behandelen documenten, die na de vergadering aan de CIU worden teruggegeven.

*Artikel 12*

**Archiveren van vertrouwelijke informatie**

1. In de beveiligde zone wordt voorzien in beveiligde archiveringsfaciliteiten. De CIU is verantwoordelijk voor het volgens de standaard archiveringscriteria beheren van de beveiligde archieven.

2. Gerubriceerde informatie die definitief bij de CIU is gedeponeerd, en als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau gerubriceerde informatie die bij het secretariaat van het parlementaire orgaan/de parlementaire ambtsdrager is gedeponeerd, wordt zes maanden na de laatste raadpleging en uiterlijk één jaar na de deponering ervan naar het beveiligde archief in de beveiligde zone overgebracht. „Andere vertrouwelijke informatie" wordt, voor zover zij niet bij de CIU is gedeponeerd, door het secretariaat van het parlementaire orgaan/de parlementaire ambtsdrager in kwestie gearchiveerd volgens de algemene regels voor het documentenbeheer.

3. Vertrouwelijke informatie die in het beveiligde archief wordt bewaard, mag worden geraadpleegd onder de volgende voorwaarden:

a) alleen de personen die aan de hand van hun naam, functie of kantoor worden geïdentificeerd in het begeleidende document dat werd opgesteld op het moment dat de vertrouwelijke informatie is gedeponeerd, zijn gemachtigd deze informatie te raadplegen;

b) aanvragen voor het raadplegen van vertrouwelijke informatie worden ingediend bij de CIU, die het desbetreffende document naar de beveiligde leeskamer overbrengt; en

c) de in artikel 10 vermelde procedures en voorwaarden voor het raadplegen van vertrouwelijke informatie zijn van toepassing.

*Artikel 13*

**Lager rubriceren, derubriceren en demarkeren van vertrouwelijke informatie**

1. Vertrouwelijke informatie kan alleen lager gerubriceerd, gederubriceerd of gedemarkeerd worden met voorafgaande instemming van de opsteller en, zo nodig, na bespreking met andere betrokken partijen.

2. Lagere rubricering en derubricering moeten schriftelijk bevestigd worden. De opsteller is er verantwoordelijk voor dat de geadresseerden van de wijziging op de hoogte worden gebracht; en deze geadresseerden zijn er op hun beurt verantwoordelijk voor dat de daaropvolgende geadresseerden, aan wie zij het document hebben gezonden of voor wie zij het hebben gekopieerd, van de wijziging op de hoogte worden gebracht. Zo mogelijk vermelden de opstellers op gerubriceerde documenten een datum waarop dan wel een periode of een gebeurtenis waarna de inhoud lager gerubriceerd of gederubriceerd kan worden. Zo niet, verifiëren zij de documenten uiterlijk om de vijf jaar om na te gaan of de oorspronkelijke rubricering moet worden gehandhaafd.

3. Vertrouwelijke informatie die in de beveiligde archieven wordt bewaard, wordt tijdig en uiterlijk op de 25ste verjaardag van de datum waarop de informatie is gegenereerd, onderzocht om te bepalen of deze informatie al dan niet moet worden gederubriceerd, lager gerubriceerd of gedemarkeerd. Het onderzoek en de publicatie van deze informatie vinden plaats overeenkomstig de bepalingen van Verordening (EEG, Euratom) nr. 354/83 van de Raad van 1 februari 1983 inzake het voor het publiek toegankelijk maken van de historische archieven van de Europese Economische Gemeenschap en de Europese Gemeenschap voor Atoomenergie ([1]). Derubricering wordt overeenkomstig bijlage I, deel 1, onder 10, uitgevoerd door de opsteller van de gerubriceerde informatie of door de op dat moment verantwoordelijke dienst.

4. Na de derubricering wordt de in het beveiligde archief bewaarde, inmiddels niet meer gerubriceerde informatie overgebracht naar de historische archieven van het Europees Parlement met het oog op permanente opslag en verdere behandeling volgens de toepasselijke regels.

5. Na de demarkering gelden voor de voorheen „andere vertrouwelijke informatie" de regels van het Europees Parlement voor het documentenbeheer.

*Artikel 14*

**Inbreuk op de beveiliging, verlies of compromittering van vertrouwelijke informatie**

1. Een inbreuk op de vertrouwelijkheid in het algemeen, en op dit besluit in het bijzonder, leidt in het geval van leden van het Europees Parlement tot de toepassing van de desbetreffende bepalingen inzake sancties, zoals opgenomen in het Reglement van het Europees Parlement.

2. Een inbreuk die is begaan door een personeelslid van het Europees Parlement, leidt tot de toepassing van de procedures en de sancties die zijn voorzien in het Statuut van de ambtenaren respectievelijk de regeling welke van toepassing is op de andere personeelsleden van de Europese Unie, zoals vastgelegd in Verordening (EEG, Euratom, EGKS) nr. 259/68 ([2]) („het Statuut").

([1]) PB L 43 van 15.2.1983, blz. 1.
([2]) PB L 56 van 4.3.1968, blz. 1.

3. De Voorzitter en/of de secretaris-generaal, naargelang van het geval, organiseren in geval van een inbreuk als omschreven in veiligheidsmededeling 6, het eventueel noodzakelijke onderzoek.

4. Indien de vertrouwelijke informatie door een andere -instelling van de Unie of door een lidstaat aan het Europees Parlement is meegedeeld, stellen de Voorzitter en/of de secretaris-generaal, naargelang van het geval, de betrokken instelling van de Unie of lidstaat op de hoogte van bewezen of vermoedelijk verlies of compromittering van gerubriceerde informatie alsmede van de resultaten van het onderzoek en de maatregelen die zijn genomen om herhaling te voorkomen.

*Artikel 15*

**Aanpassing van dit besluit en de uitvoeringsregels en jaarlijkse rapportage over de toepassing van dit besluit**

1. De secretaris-generaal doet de nodige voorstellen voor de aanpassing van dit besluit en de uitvoeringsregels in de bijlagen, en legt deze voorstellen voor aan het Bureau voor een besluit.

2. De secretaris-generaal is verantwoordelijk voor de toepassing van dit besluit door de diensten van het Europees Parlement en vaardigt overeenkomstig de in dit besluit verankerde beginselen instructies uit voor de behandeling van zaken die onder het ISMS vallen.

3. De secretaris-generaal doet het Bureau een jaarverslag over de toepassing van dit besluit toekomen.

*Artikel 16*

**Overgangsbepalingen en slotbepalingen**

1. Niet-gerubriceerde informatie die wordt bewaard bij de CIU of in een ander archief van het Europees Parlement, en die als vertrouwelijk wordt beschouwd en vóór 1 april 2014 gedateerd is, wordt voor de toepassing van dit besluit „andere vertrouwelijke informatie" geacht te zijn. De opsteller kan de graad van vertrouwelijkheid ervan te allen tijde herzien.

2. In afwijking van artikel 5, lid 1, onder a), en van artikel 8, lid 1, van dit besluit wordt gedurende een periode van twaalf maanden, te rekenen vanaf 1 april 2014, door de Raad uit hoofde van het Interinstitutioneel Akkoord verstrekte informatie die als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau gerubriceerd is, gedeponeerd bij, geregistreerd door en opgeslagen in de CIU. Deze informatie kan overeenkomstig artikel 4, lid 4, onder a) en c), en artikel 5, lid 4, van het Interinstitutioneel Akkoord worden geraadpleegd.

3. Het besluit van het Bureau van 6 juni 2011 over de regels voor de behandeling van vertrouwelijke informatie door het Europees Parlement wordt ingetrokken.

*Artikel 17*

**Inwerkingtreding**

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

*BIJLAGE I*

**Deel 1**

**BASISBEGINSELEN EN MINIMUMNORMEN INZAKE VEILIGHEID VOOR DE BESCHERMING VAN VERTROUWELIJKE INFORMATIE**

1. **INLEIDING**

Deze voorschriften bevatten de grondbeginselen en minimumnormen inzake veiligheid voor de bescherming van vertrouwelijke informatie die door het Europees Parlement in al zijn standplaatsen en door alle ontvangers van gerubriceerde informatie en „andere vertrouwelijke informatie" moeten worden in acht genomen en/ofnageleefd, zodat de veiligheid wordt gegarandeerd en alle betrokkenen er zeker van kunnen zijn dat er een gemeenschappelijke norm voor de bescherming geldt. Deze voorschriften worden aangevuld met de in bijlage II vervatte veiligheidsmededelingen en met andere bepalingen betreffende de verwerking van vertrouwelijke informatie door parlementaire commissies en andere parlementaire organen/ambtsdragers.

2. **BASISBEGINSELEN**

Het veiligheidsbeleid van het Europees Parlement maakt integraal onderdeel uit van zijn algemeen beleid inzake intern beheer en is dus gebaseerd op de beginselen van dat algemeen beleid. Deze beginselen zijn: wettigheid, transparantie, verantwoordingsplicht, subsidiariteit en proportionaliteit.

Wettigheid houdt in dat de uitoefening van veiligheidsfuncties strikt binnen het geldende rechtskader moeten worden uitgeoefend en dat de toepasselijke regelgeving moet worden nageleefd. Voorts moeten de verantwoordelijkheden op veiligheidsgebied gebaseerd zijn op adequate rechtsvoorschriften. Het Statuut is volledig van toepassing, in het bijzonder artikel 17 inzake de verplichting van de personeelsleden om zich te onthouden van het niet-geautoriseerde openbaar maken van informatie die in dienst is ontvangen, en titel VI inzake tuchtmaatregelen. Ten slotte worden veiligheidsinbreuken die onder de verantwoordelijkheid van het Europees Parlement vallen, behandeld op een wijze die strookt met zijn Reglement en zijn beleid inzake tuchtmaatregelen.

Transparantie houdt in dat alle veiligheidsvoorschriften en -bepalingen duidelijk moeten zijn, dat er een evenwicht moet bestaan tussen de verschillende diensten en de verschillende gebieden (fysieke veiligheid in verhouding tot de bescherming van gegevens, enz.) en dat een coherent en gestructureerd beleid inzake veiligheidsbewustzijn moet worden gevoerd. Voorts zijn duidelijke schriftelijke richtsnoeren nodig voor de uitvoering van de veiligheidsmaatregelen.

Verantwoordingsplicht houdt in dat de verantwoordelijkheden op het gebied van de veiligheid duidelijk moeten worden vastgesteld. Voorts houdt dit beginsel in dat regelmatig moet worden nagegaan of deze verantwoordelijkheden correct zijn uitgeoefend.

Subsidiariteit betekent dat de veiligheid op het laagst mogelijke niveau moet worden georganiseerd en zo dicht mogelijk bij de Directoraten-generaal en de diensten van het Europees Parlement. Proportionaliteit houdt in dat de beveiligingsactiviteiten strikt worden beperkt tot hetgeen absoluut noodzakelijk is en dat de veiligheidsmaatregelen in verhouding moeten staan tot de te beschermen belangen en tot de feitelijke of mogelijke bedreiging van deze belangen, zodat deze belangen op een zodanige wijze kunnen worden beschermd dat zo weinig mogelijk ontwrichting wordt veroorzaakt.

3. **FUNDAMENTEN VOOR GEGEVENSBEVEILIGING**

De fundamenten voor een goede gegevensbeveiliging zijn:

a) goede communicatie- en informatiesystemen (CIS). Die vallen, onder de verantwoordelijkheid van de veiligheidsautoriteit van het Europees Parlement (zoals omschreven in veiligheidsmededeling 1);

b) de aanwezigheid in het Europees Parlement van de instantie voor informatieborging (information assurance, hierna „IA"), die met de betrokken veiligheidsautoriteit (zoals omschreven in veiligheidsmededeling 1) samenwerkt om informatie en advies te verschaffen over technische bedreigingen voor de CIS en over de middelen om zich tegen die bedreigingen te beschermen;

c) nauwe samenwerking tussen de verantwoordelijke diensten van het Europees Parlement en de veiligheidsdiensten van de overige instellingen van de Unie;

4. **BEGINSELEN VAN DE GEGEVENSBEVEILIGING**

4.1. ***Doelstellingen***

De hoofddoelstellingen van gegevensbeveiliging zijn als volgt:

a) beveiliging van vertrouwelijke informatie tegen spionage, compromittering of openbaarmaking zonder machtiging;

b) beveiliging van gerubriceerde informatie die in communicatie- en informatiesystemen en -netwerken wordt verwerkt, tegen gevaren met betrekking tot het vertrouwelijke karakter, de integriteit en de beschikbaarheid ervan;

c) beveiliging van de locaties van het Europees Parlement waar gerubriceerde informatie is ondergebracht, tegen sabotage en kwaadwillige beschadiging;

d) in geval van een veiligheidsinbreuk, beoordeling van de aangerichte schade, beperking van de gevolgen ervan, uitvoering van een veiligheidsonderzoek en vaststelling van eventueel noodzakelijke corrigerende maatregelen.

4.2. ***Rubricering***

4.2.1. Waar vertrouwelijkheid van belang is, zijn zorg en ervaring nodig bij de selectie van de informatie en het materiaal die moeten worden beschermd en bij de beoordeling van de mate van vereiste bescherming. Het is van essentieel belang dat de mate van bescherming overeenstemt met de gevoeligheid in termen van beveiliging van de te beschermen informatie of het materiaal. Om voor een soepele informatiestroom te zorgen, moeten zowel een te hoge als een te lage rubricering worden voorkomen.

4.2.2. Het rubriceringssysteem is het instrument waarmee gevolg wordt gegeven aan de beginselen die in dit deel uiteen worden gezet. Een soortgelijk rubriceringssysteem moet worden gebruikt voor het plannen en organiseren van de bestrijding van spionage, sabotage, terrorisme en andere bedreigingen, zodat de grootste mate van bescherming gewaarborgd is voor de belangrijkste locaties waar gerubriceerde informatie is ondergebracht, en binnen die locaties voor de gevoeligste elementen.

4.2.3. Voor de rubricering van informatie is alleen de opsteller van de betreffende informatie verantwoordelijk.

4.2.4. Het rubriceringsniveau mag uitsluitend worden bepaald op basis van de inhoud van de informatie in kwestie.

4.2.5. Als afzonderlijke gegevens worden bijeengebracht, moet voor het geheel een rubriceringsniveau gelden dat minstens even hoog is als de hoogste rubricering van een van die gegevens. Aan een informatieverzameling kan evenwel een hogere rubricering worden toegekend dan aan de bestanddelen ervan.

4.2.6 Rubricering wordt alleen toegekend als dit nodig is en zolang als dit nodig is.

4.3. ***Doel van de veiligheidsmaatregelen***

De veiligheidsmaatregelen moeten:

a) betrekking hebben op alle personen die toegang hebben tot gerubriceerde informatie, dragers van gerubriceerde informatie en „andere vertrouwelijke informatie", alsmede op alle locaties waar zich deze informatie bevindt en belangrijke installaties;

b) zodanig ontworpen zijn dat personen worden gedetecteerd wier positie (in de zin van toegang, relaties of anderszins) de veiligheid van de bedoelde informatie en van belangrijke installaties waar deze informatie is ondergebracht, in gevaar kan brengen, en moeten in de uitsluiting of verwijdering van deze personen voorzien;

c) voorkomen dat een niet-gemachtigde persoon toegang krijgt tot de bedoelde informatie of tot installaties die deze informatie bevatten;

d) ervoor zorgen dat de bedoelde informatie alleen verspreid wordt op basis van het „need to know"-beginsel, dat fundamenteel is voor alle aspecten van de veiligheid;

e) waarborgen bieden voor de integriteit (d.w.z. het voorkomen van schending of van wijziging of verwijdering van informatie zonder machtiging) en de beschikbaarheid (d.w.z. dat de toegang niet geweigerd wordt aan degene die de informatie nodig heeft en tot toegang gemachtigd is) van vertrouwelijke informatie en in het bijzonder van informatie die in elektromagnetische vorm wordt opgeslagen, verwerkt of verzonden.

## 5. GEMEENSCHAPPELIJKE MINIMUMNORMEN

Het Europees Parlement zorgt ervoor dat gemeenschappelijke minimumnormen inzake veiligheid in acht worden genomen door alle ontvangers van gerubriceerde informatie, zowel in de instelling als onder haar bevoegdheid vallend, namelijk alle diensten en contractanten, zodat deze informatie kan worden doorgegeven in het vertrouwen dat zij met dezelfde zorg zal worden behandeld. Deze minimumnormen omvatten criteria voor de veiligheidsmachtiging van ambtenaren van het Europees Parlement en andere parlementaire medewerkers die in dienst van een fractie zijn, en procedures voor de bescherming van vertrouwelijke informatie.

Het Europees Parlement verleent derden alleen toegang tot de bedoelde informatie als zij garanderen dat deze informatie wordt behandeld in overeenstemming met voorschriften die minstens volstrekt gelijkwaardig aan deze gemeenschappelijke minimumnormen zijn.

Dergelijke gemeenschappelijke minimumnormen moeten ook worden toegepast, wanneer het Europees Parlement uit hoofde van een opdracht of een subsidieovereenkomst taken aan industriële of andere entiteiten toekent, waarbij vertrouwelijke informatie in het geding is.

## 6. VEILIGHEID BETREFFENDE AMBTENAREN VAN HET EUROPEES PARLEMENT EN ANDERE PARLEMENTAIRE MEDEWERKERS DIE IN DIENST VAN EEN FRACTIE ZIJN

### 6.1. *Veiligheidsinstructies betreffende ambtenaren van het Europees Parlement en andere parlementaire medewerkers die in dienst van een fractie zijn*

Ambtenaren van het Europees Parlement en andere parlementaire medewerkers die in dienst van een fractie zijn, in functies waardoor zij toegang kunnen hebben tot gerubriceerde informatie, krijgen bij ambtsaanvaarding en daarna met regelmatige tussenpozen grondige instructies over de noodzaak van beveiliging en de betrokken procedures. Deze personen moeten schriftelijk bevestigen dat zij de toepasselijke bepalingen inzake veiligheid hebben gelezen en volledig hebben begrepen.

### 6.2. *Verantwoordelijkheden van leidinggevenden*

Leidinggevenden hebben onder meer de taak te weten welke leden van hun personeel bij werkzaamheden betreffende vertrouwelijke informatie betrokken zijn of toegang hebben tot beveiligde communicatie- of informatiesystemen, en incidenten of manifeste zwakke plekken die gevolgen voor de veiligheid kunnen hebben, te registreren en te melden.

### 6.3. *Veiligheidsstatus van ambtenaren en andere parlementaire medewerkers die in dienst van een fractie zijn*

Er worden procedures ingesteld om ervoor te zorgen dat, wanneer negatieve informatie bekend wordt over een ambtenaar van het Europees Parlement of een andere parlementaire medewerker die in dienst van een fractie is, stappen worden ondernomen om vast te stellen of het werk van deze persoon hem of haar in contact heeft gebracht met gerubriceerde informatie en of hij of zij toegang heeft tot beveiligde communicatie- of informatiesystemen, en dat de bevoegde dienst van het Europees Parlement wordt ingelicht. Als de bevoegde nationale veiligheidsautoriteit aangeeft dat de bedoelde persoon een veiligheidsrisico vormt, wordt hij of zij uitgesloten of ontheven van taken waarin hij of zij de veiligheid in gevaar kan brengen.

## 7. FYSIEKE VEILIGHEID

Fysieke veiligheid houdt in: de toepassing van fysieke en technische beschermingsmaatregelen om niet-geautoriseerde toegang tot gerubriceerde informatie te voorkomen.

7.1. ***Noodzaak van bescherming***

Het niveau van de fysieke beveiligingsmaatregelen die moeten worden toegepast om de bescherming van gerubriceerde informatie te waarborgen, moet in verhouding staan tot de rubricering en de omvang van, en de bedreiging voor, de aanwezige informatie en het aanwezige materiaal. Alle houders van gerubriceerde informatie volgen voor de rubricering van die informatie uniforme praktijken en moeten voldoen aan gemeenschappelijke beschermingsnormen met betrekking tot bewaring, overdracht en verwijdering van informatie en materiaal die moeten worden beschermd.

7.2. ***Controle***

Alvorens zones die gerubriceerde informatie bevatten onbemand achter te laten, moeten personen die met de bewaring zijn belast, ervoor zorgen dat de informatie veilig is opgeborgen en dat alle beveiligingsmiddelen (sloten, alarm enz.) geactiveerd zijn. Aanvullende onafhankelijke controles worden na afloop van de werktijden uitgevoerd.

7.3. ***Beveiliging van gebouwen***

Gebouwen waarin gerubriceerde informatie of beveiligde communicatie- en informatiesystemen zijn gehuisvest, moeten tegen ongeoorloofde toegang worden beschermd.

De aard van de bescherming die voor gerubriceerde informatie wordt gebruikt, bijvoorbeeld tralies voor vensters, deursloten, bewakers bij de ingangen, automatische toegangscontrolesystemen, veiligheidscontroles en -patrouilles, alarmsystemen, indringerdetectiesystemen en waakhonden, hangt af van:

a) de rubricering, het volume en de locatie binnen het gebouw, van de te beschermen informatie en het materiaal;

b) de kwaliteit van de opbergmiddelen voor de beveiliging van de betreffende informatie en het betreffende materiaal; en

c) de fysieke aard en locatie van het gebouw.

De aard van de bescherming die voor communicatie- en informatiesystemen wordt gebruikt, hangt af van een beoordeling van de waarde van deze systemen en de potentiële schade als de veiligheid gecompromitteerd zou worden, de fysieke aard en locatie van het gebouw waar het systeem is ondergebracht, en van de locatie van dat systeem binnen het gebouw.

7.4. ***Noodplannen***

Er worden vooraf gedetailleerde plannen opgesteld voor de bescherming van gerubriceerde informatie in noodsituaties.

8. **BEVEILIGINGSINDICATOREN, MARKERINGEN, HET AANBRENGEN EN HET BEHEER VAN RUBRICERINGEN**

8.1. ***Beveiligingsindicatoren***

Andere rubriceringen dan die welke in artikel 2, onder d), van dit besluit zijn gedefinieerd, zijn niet toegestaan.

Een overeengekomen beveiligingsindicator mag worden gebruikt om de geldigheidsduur van een rubricering te beperken (wat voor gerubriceerde informatie inhoudt dat zij automatisch lager wordt gerubriceerd of wordt gederubriceerd).

Beveiligingsindicatoren mogen alleen worden gebruikt in combinatie met een rubricering.

De beveiligingsindicatoren worden nader geregeld in veiligheidsmededeling 2 en gedefinieerd in de instructies voor behandeling.

8.2. ***Markeringen***

Een markering wordt gebruikt om van tevoren omschreven specifieke instructies voor de verwerking van vertrouwelijke informatie te specificeren. Markeringen kunnen ook aangeve***n*** op welk domein een document betrekking heeft, dat er een speciale verspreiding op een „need to know"-basis plaatsvindt of (voor niet-gerubriceerde informatie) dat een publicatieverbod afloopt.

Een markering is geen rubricering en mag niet in plaats daarvan worden gebruikt.

De markeringen worden nader geregeld in veiligheidsmededeling 2 en gedefinieerd in de instructies voor behandeling.

8.3. ***Aanbrengen van een rubricering en van beveiligingsindicatoren***

Een rubricering en beveiligingsindicatoren en markeringen worden aangebracht overeenkomstig veiligheidsmededeling 2, afdeling E, en de instructies voor behandeling.

8.4. ***Beheer van de rubriceringen***

8.4.1 *Algemeen*

Informatie wordt alleen gerubriceerd wanneer dat noodzakelijk is. De rubricering moet duidelijk en correct worden aangegeven en mag slechts gehandhaafd worden zolang de informatie beschermd moet worden.

De verantwoordelijkheid voor het rubriceren van gegevens en een eventuele lagere rubricering of derubricering nadien, berust uitsluitend bij de opsteller.

Ambtenaren van het Europees Parlement rubriceren informatie, geven deze een lagere rubricering of derubriceren deze op instructie van of krachtens een delegatie van de secretaris-generaal.

De gedetailleerde procedures voor de behandeling van gerubriceerde documenten zijn zo opgezet dat zij een bescherming bieden die passend is voor de inhoud van die documenten.

Het aantal personen dat gemachtigd is om informatie te genereren die gerubriceerd is als „TRÈS SECRET UE/EU TOP SECRET", wordt tot een minimum beperkt, en hun namen worden op een lijst geplaatst die door de CIU wordt bijgehouden.

8.4.2 *Rubricering*

Het rubriceringsniveau van een document wordt bepaald door het niveau van gevoeligheid van de inhoud, overeenkomstig de definities in artikel 2, onder d). Het is van belang dat rubriceringen correct en terughoudend worden toegekend.

De rubricering van een brief of nota die bijvoegsels bevat, is ten minste even hoog als die van het hoogst gerubriceerde bijvoegsel. De opsteller moet duidelijk aangeven welke rubricering op de brief of nota moet worden toegepast indien deze van de bijvoegsels wordt gescheiden.

De opsteller van een te rubriceren document houdt rekening met de hierboven uiteengezette regels en vermijdt te hoge of te lage rubriceringen.

Afzonderlijke bladzijden, punten, afdelingen, bijlagen, aanhangsels, aanhechtsels en bijvoegsels van een bepaald document kunnen verschillende rubriceringen vereisen en moeten dienovereenkomstig gerubriceerd worden. De rubricering die voor het gehele document geldt, is in dat geval die van het hoogst gerubriceerde gedeelte.

9. **INSPECTIES**

Er worden periodieke interne inspecties van de maatregelen voor de beveiliging van gerubriceerde informatie uitgevoerd door het directoraat Veiligheid en risicobeoordeling van het Europees Parlement, dat de veiligheidsautoriteiten van de Raad of de Commissie om bijstand kan verzoeken.

De veiligheidsautoriteiten en de bevoegde diensten van de instellingen van de Unie kunnen in het kader van een onderling overeengekomen proces op initiatief van een van de partijen de maatregelen voor de beveiliging van gerubriceerde informatie die uit hoofde van de relevante interinstitutionele akkoorden wordt uitgewisseld, aan collegiale toetsingen onderwerpen.

10. **PROCEDURES VOOR DERUBRICERING EN DEMARKERING**

10.1. De CIU onderzoekt uiterlijk op de 25ste verjaardag van het opstellen van een document, de vertrouwelijke informatie in haar register en verzoekt de opsteller om toestemming voor derubricering of demarkering van dat document. Documenten die niet bij het eerste onderzoek zijn gederubriceerd of gedemarkeerd, worden op gezette tijden, maar ten minste om de vijf jaar, opnieuw onderzocht. Naast de documenten die zich daadwerkelijk in de beveiligde archieven in de beveiligde zone bevinden en naar behoren zijn gerubriceerd, kan het demarkeringsproces ook betrekking hebben op andere vertrouwelijke informatie die bij het parlementair orgaan/ambt bewaard wordt dan wel in de dienst die de historische archieven van het Parlement beheert.

10.2. Het besluit tot derubricering of demarkering van een document wordt als algemene regel alleen door de opsteller genomen of bij wijze van uitzondering in samenwerking met het parlementair orgaan/ambt dat houder van de betrokken informatie is, voordat de in het document vervatte informatie wordt overgedragen aan de dienst die de historische archieven van het Parlement beheert. Derubricering of demarkering van gerubriceerde informatie mag alleen met voorafgaande schriftelijke toestemming van de opsteller plaatsvinden. In het geval van „andere vertrouwelijke informatie"beslist het secretariaat van het parlementaire orgaan dat/de parlementaire ambtsdrager die houder van de betrokken informatie is, in samenwerking met de opsteller of het document kan worden gedemarkeerd.

10.3. De CIU is er namens de opsteller verantwoordelijk voor dat de geadresseerden van het document van de wijziging in de rubricering of markering op de hoogte worden gebracht, en deze geadresseerden zijn er op hun beurt verantwoordelijk voor dat de daaropvolgende geadresseerden, aan wie zij het document hebben toegezonden of voor wie zij het gekopieerd hebben, van de wijziging op de hoogte worden gebracht.

10.4. Derubricering heeft geen gevolgen voor eventuele beveiligingsindicatoren of markeringen die op het document zichtbaar zijn.

10.5. In geval van derubricering wordt de oorspronkelijke rubricering boven- en onderaan elke pagina doorgehaald. De eerste pagina (schutblad) van het document wordt afgestempeld en de referentie van de CIU wordt erop aangebracht. In geval van demarkering wordt de oorspronkelijke markering bovenaan elke pagina doorgehaald.

10.6. De tekst van het gederubriceerde of gedemarkeerde document wordt gehecht aan de elektronische fiche of het equivalente systeem waar het is geregistreerd.

10.7. In het geval van documenten die vallen onder de uitzondering betreffende de persoonlijke levenssfeer en de integriteit van het individu, of de uitzondering betreffende de commerciële belangen van natuurlijke en rechtspersonen, en in het geval van gevoelige documenten geldt artikel 2 van Verordening (EEG, Euratom) nr. 354/83 van de Raad.

10.8. Naast het in de punten 10.1 tot en met 10.7 bepaalde gelden de volgende regels:

a) ten aanzien van documenten van derden raadpleegt de CIU de derde alvorens tot derubricering of demarkering over te gaan;

b) in verband met de uitzondering betreffende de persoonlijke levenssfeer en de integriteit van het individu zal bij de procedure voor derubricering of demarkering in het bijzonder rekening worden gehouden met de instemming van de persoon in kwestie dan wel de onmogelijkheid de persoon in kwestie te identificeren;

c) in verband met de uitzondering betreffende de commerciële belangen van een natuurlijke of rechtspersoon kan de persoon in kwestie op de hoogte worden gebracht via publicatie in het *Publicatieblad van de Europese Unie*, met een tijdslimiet van vier weken vanaf de datum van publicatie voor eventuele opmerkingen.

**Deel 2**

**PROCEDURE VOOR HET VEILIGHEIDSONDERZOEK**

11. **VEILIGHEIDSONDERZOEK VOOR LEDEN VAN HET EUROPEES PARLEMENT**

11.1. Om toegang te krijgen tot als „CONFIDENTIEL UE/EU CONFIDENTIAL" of op een gelijkwaardig niveau gerubriceerde informatie, moeten de leden van het Europees Parlement gemachtigd zijn hetzij volgens de in de punten 11.3 en 11.4 van deze bijlage bedoelde procedure, hetzij op basis van een plechtige verklaring inzake niet-openbaarmaking, als bedoeld in artikel 3, lid 4, van dit besluit.

11.2 Om toegang te krijgen tot als „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau gerubriceerde informatie, moeten de leden van het Europees Parlement gemachtigd zijn volgens de in de punten 11.3 en 11.14 bedoelde procedure.

11.3. Machtiging wordt alleen verleend aan leden van het Europees Parlement die een veiligheidsonderzoek door de bevoegde nationale instanties van de lidstaten hebben ondergaan in overeenstemming met de in de punten 11.9 tot en met 11.14 bedoelde procedure. De Voorzitter is verantwoordelijk voor het verlenen van machtiging aan de leden.

11.4 De Voorzitter kan een schriftelijke machtiging verlenen na verkrijging van het advies van de bevoegde nationale instanties van de lidstaten, dat gebaseerd is op het veiligheidsonderzoek dat overeenkomstig de punten 11.8 tot en met 11.13 is uitgevoerd.

11.5. Het directoraat Veiligheid en risicobeoordeling van het Europees Parlement houdt een bijgewerkte lijst bij van alle leden van het Europees Parlement aan wie een machtiging is verleend, inclusief een voorlopige machtiging in de zin van punt 11.15.

11.6. De machtiging wordt verleend voor een periode van vijf jaar of voor de duur van de taken waarvoor de machtiging verleend is, als die periode korter is. Zij kan worden verlengd volgens de in punt 11.4 bedoelde procedure.

11.7. Een machtiging wordt door de Voorzitter ingetrokken, als hij van mening is dat er voor de intrekking gegronde redenen zijn. Van een besluit tot intrekking van een machtiging wordt kennis gegeven aan het lid van het Europees Parlement in kwestie, dat kan verzoeken door de Voorzitter te worden gehoord voordat de intrekking van kracht wordt, en aan de bevoegde nationale instantie.

11.8. Een veiligheidsonderzoek wordt uitgevoerd met de medewerking van het lid van het Europees Parlement in kwestie en op verzoek van de Voorzitter. De nationale instantie van de lidstaat waarvan het betrokken lid onderdaan is, is bevoegd om het onderzoek uit te voeren.

11.9. Als onderdeel van het veiligheidsonderzoek moet het lid van het Europees Parlement in kwestie een formulier met persoonlijke gegevens invullen.

11.10. De Voorzitter specificeert in zijn verzoek aan de bevoegde nationale instantie het niveau van de gerubriceerde informatie waartoe het lid in kwestie toegang moet krijgen, zodat zij het veiligheidsonderzoek kan uitvoeren.

11.11 Het gehele veiligheidsonderzoek dat door de bevoegde nationale instantie wordt uitgevoerd, samen met het verkregen resultaat, moet voldoen aan de ter zake vigerende voorschriften in de lidstaat in kwestie, inclusief de regels inzake beroep.

11.12. Als de bevoegde nationale instantie een positief advies uitbrengt, mag de Voorzitter het lid van het Europees Parlement in kwestie de machtiging verlenen.

11.13. Een negatief advies van de bevoegde nationale instantie wordt ter kennis gebracht van het lid van het Europees Parlement in kwestie, dat mag vragen te worden gehoord door de Voorzitter. Als de Voorzitter het nodig acht, kan hij de bevoegde nationale instantie om een nadere toelichting verzoeken. Indien het negatief advies wordt bevestigd, wordt geen machtiging verleend.

11.14. Alle leden van het Europees Parlement aan wie machtiging wordt verleend als bedoeld in punt 11.3, ontvangen op het tijdstip dat de machtiging wordt verleend en vervolgens met regelmatige tussenpozen, alle noodzakelijke richtsnoeren over de bescherming van gerubriceerde informatie en de wijze waarop deze bescherming kan worden gewaarborgd. Die leden ondertekenen een verklaring waarin zij de ontvangst van deze richtsnoeren bevestigen.

11.15. In uitzonderlijke omstandigheden mag de Voorzitter, nadat hij de bevoegde nationale instantie heeft geïnformeerd en mits die instantie niet binnen een maand heeft gereageerd, aan een lid van het Europees Parlement een voorlopige machtiging voor een periode van hoogstens zes maanden verlenen, in afwachting van het resultaat van het onderzoek als bedoeld in punt 11.11. De voorlopige machtiging die aldus wordt verleend, geeft geen toegang tot informatie die als „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd.

12. **VEILIGHEIDSONDERZOEK VOOR AMBTENAREN VAN HET EUROPEES PARLEMENT EN ANDERE PARLEMENTAIRE MEDEWERKERS DIE IN DIENST VAN EEN FRACTIE ZIJN**

12.1. Alleen ambtenaren van het Europees Parlement en andere parlementaire medewerkers in dienst van een fractie die wegens hun functie en de eisen van hun dienst kennis moeten nemen of gebruik moeten maken van gerubriceerde informatie, krijgen toegang tot die informatie.

12.2. Om toegang te krijgen tot informatie die als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd, moeten de ambtenaren van het Europees Parlement en andere parlementaire medewerkers die in dienst van een fractie zijn, gemachtigd zijn volgens de in de punten 12.3 en 12.4 bedoelde procedure.

12.3. Machtiging wordt alleen verleend aan de in punt 12.1 genoemde personen die een veiligheidsonderzoek door de bevoegde nationale instanties van de lidstaten hebben ondergaan in overeenstemming met de in de punten 12.9 tot en met 12.14 bedoelde procedure. De secretaris-generaal is verantwoordelijk voor het verlenen van machtiging aan ambtenaren van het Europees Parlement en andere parlementaire medewerkers die in dienst van een fractie zijn.

12.4 De secretaris-generaal kan een schriftelijke machtiging verlenen na verkrijging van het advies van de bevoegde nationale instanties van de lidstaten, dat gebaseerd is op het veiligheidsonderzoek dat overeenkomstig de punten 12.8 tot en met 12.13 is uitgevoerd.

12.5. Het directoraat Veiligheid en risicobeoordeling van het Europees Parlement houdt een bijgewerkte lijst bij van alle posten waarvoor een veiligheidsmachtiging vereist is, zoals aangegeven door de betrokken diensten van het Europees Parlement, alsmede een lijst van alle personen aan wie een machtiging, inclusief een tijdelijke machtiging als bedoeld in punt 12.15, is verleend.

12.6. De machtiging wordt verleend voor een periode van vijf jaar of voor de duur van de taken waarvoor de machtiging verleend is, als die periode korter is. Zij kan worden verlengd volgens de in punt 12.4 bedoelde procedure.

12.7. Een machtiging wordt door de secretaris-generaal ingetrokken, als hij van mening is dat voor de intrekking gegronde redenen zijn. Van een besluit tot intrekking van een machtiging wordt kennis gegeven aan de betreffende ambtenaar van het Europees Parlement of aan de betreffende parlementaire medewerker in dienst van een fractie, die kan verzoeken om door de secretaris-generaal te worden gehoord voordat de intrekking van kracht wordt, en aan de bevoegde nationale instantie.

12.8. Een veiligheidsonderzoek wordt uitgevoerd met de medewerking van de betrokken ambtenaar van het Europees Parlement of andere parlementaire medewerker in dienst van een fractie en op verzoek van de secretaris-generaal. De nationale instantie van de lidstaat waarvan de betrokkene onderdaan is, is bevoegd om het onderzoek uit te voeren. Als de nationale wet- en regelgeving dit toestaan, mogen de bevoegde nationale instanties onderzoek uitvoeren naar niet-onderdanen die toegang moeten krijgen tot informatie die als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" is gerubriceerd.

12.9. Als onderdeel van het veiligheidsonderzoek moet de betreffende ambtenaar van het Europees Parlement of andere parlementaire medewerker die in dienst van een fractie is, een formulier met persoonlijke gegevens invullen.

12.10. De secretaris-generaal specificeert in zijn/haar verzoek aan de bevoegde nationale instantie het niveau van de gerubriceerde informatie waartoe de betrokken ambtenaar van het Europees Parlement of andere parlementaire medewerker in dienst van een fractie toegang moet krijgen, zodat zij het veiligheidsonderzoek kan uitvoeren en hun advies kan geven over het machtigingsniveau dat voor de persoon in kwestie geschikt is.

12.11. Het gehele veiligheidsonderzoek dat door de bevoegde nationale instantie wordt uitgevoerd, samen met het verkregen resultaat, moet voldoen aan de ter zake vigerende voorschriften in de lidstaat in kwestie, inclusief de regels inzake beroep.

12.12. Als de bevoegde nationale instantie van de lidstaat een positief advies uitbrengt, mag de secretaris-generaal de betrokken ambtenaar van het Europees Parlement of andere parlementaire medewerker in dienst van een fractie de machtiging verlenen.

12.13. Een negatief advies van de bevoegde nationale instantie wordt ter kennis gebracht van de betreffende ambtenaar van het Europees Parlement of andere parlementaire medewerker in dienst van een fractie, die mag vragen te worden gehoord door de secretaris-generaal. Als de secretaris-generaal het nodig acht, kan hij de bevoegde nationale instantie om een nadere toelichting verzoeken. Indien het negatief advies wordt bevestigd, wordt geen machtiging verleend.

12.14. Alle ambtenaren van het Europees Parlement en andere parlementaire medewerkers in dienst van een fractie aan wie machtiging wordt verleend in de zin van de punten 12.4 en 12.5, ontvangen op het tijdstip dat de machtiging wordt verleend en vervolgens met regelmatige tussenpozen, alle noodzakelijke richtsnoeren betreffende de bescherming van gerubriceerde informatie en de wijze waarop deze bescherming kan worden gewaarborgd. Die ambtenaren en medewerkers ondertekenen een verklaring waarin zij de ontvangst van deze richtsnoeren bevestigen en zich ertoe verplichten deze op te volgen.

12.15. In uitzonderlijke omstandigheden mag de secretaris-generaal, nadat hij de nationale bevoegde instantie heeft geïnformeerd en mits deze niet binnen een maand heeft gereageerd, aan een ambtenaar van het Parlement of andere parlementaire medewerker die in dienst van een fractie is, een voorlopige machtiging verlenen voor een periode van hoogstens zes maanden, in afwachting van het resultaat van het onderzoek als bedoeld in punt 12.11. De voorlopige machtiging die aldus wordt verleend, geeft geen toegang tot informatie die als „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd.

*BIJLAGE II*

**INLEIDING**

De volgende veiligheidsmededelingen betreffen de veilige behandeling en het veilige beheer van vertrouwelijke informatie bij het Europees Parlement. Samen met de instructies voor behandeling vormen die veiligheidsmededelingen het beheerssysteem voor informatieveiligheid (ISMS) als bedoeld in artikel 3, lid 2, van dit besluit.

**VEILIGHEIDSMEDEDELING 1**

**Organisatie van de beveiliging in het Europees Parlement ter bescherming van vertrouwelijke informatie**

**VEILIGHEIDSMEDEDELING 2**

**Beheer van gerubriceerde informatie**

**VEILIGHEIDSMEDEDELING 3**

**De verwerking van vertrouwelijke informatie door middel van geautomatiseerde communicatie- en informatiesystemen (CIS)**

**VEILIGHEIDSMEDEDELING 4**

**Fysieke beveiliging**

**VEILIGHEIDSMEDEDELING 5**

**Industriële beveiliging**

**VEILIGHEIDSMEDEDELING 6**

**Inbreuk op de beveiliging, verlies of compromittering van gerubriceerde informatie**

**VEILIGHEIDSMEDEDELING 1**

ORGANISATIE VAN DE BEVEILIGING IN HET EUROPEES PARLEMENT TER BESCHERMING VAN VERTROUWELIJKE INFORMATIE

1. De secretaris-generaal is verantwoordelijk voor de algemene en consistente uitvoering van dit besluit.

De secretaris-generaal neemt de nodige maatregelen om ervoor te zorgen dat dit besluit bij de behandeling of opslag van vertrouwelijke informatie in de gebouwen van het Europees Parlement wordt toegepast door leden van het Europees Parlement, ambtenaren van het Europees Parlement, andere parlementaire medewerkers die in dienst van een fractie is en contractanten.

2. De secretaris-generaal is de veiligheidsinstantie (SA). In deze hoedanigheid is de secretaris-generaal verantwoordelijk voor de volgende taken:

2.1. hij coördineert alle beveiligingskwesties in verband met de activiteiten van het Parlement wat de bescherming van vertrouwelijke informatie betreft;

2.2. hij keurt de instelling van een beveiligde zone, beveiligde leeskamers en beveiligde apparatuur goed;

2.3. hij past besluiten toe waarbij het Parlement krachtens artikel 6 van dit besluit wordt toegestaan gerubriceerde informatie aan derden toe te zenden;

2.4. hij onderzoekt of gelast een onderzoek naar lekken van gerubriceerde informatie die zich op het eerste gezicht bij het Parlement hebben voorgedaan, in overleg met de Voorzitter van het Europees Parlement indien er een lid van het Europees Parlement bij betrokken is;

2.5. hij onderhoudt nauwe contacten met de veiligheidsinstanties van andere instellingen van de Unie en met nationale veiligheidsinstanties in de lidstaten met het oog op een optimale coördinatie van het beveiligingsbeleid inzake gerubriceerde informatie;

2.6. hij houdt het beleid en de procedures van het Parlement inzake beveiliging voortdurend in het oog en doet naar aanleiding daarvan passende aanbevelingen;

2.7. hij brengt verslag uit aan de nationale veiligheidsinstantie (NSA) die het veiligheidsonderzoek overeenkomstig bijlage I, deel 2, punt 11.3, heeft uitgevoerd indien er negatieve informatie bekend wordt die voor die instantie van belang is.

3. Indien er een lid van het Europees Parlement betrokken is, oefent de secretaris-generaal zijn verantwoordelijkheden uit in nauw overleg met de Voorzitter van het Europees Parlement;

4. Bij de uitoefening van zijn verantwoordelijkheden krachtens de leden 2 en 3 wordt de secretaris-generaal bijgestaan door de adjunct-secretaris-generaal, het directoraat Veiligheid en risicobeoordeling, het directoraat Informatietechnologie (DIT) en de afdeling Gerubriceerde gegevens (CIU).

4.1. Het directoraat Veiligheid en risicobeoordeling is verantwoordelijk voor persoonlijke beschermingsmaatregelen en met name voor de veiligheidsmachtigingsprocedure als bedoeld in bijlage I, deel 2. Het directoraat Veiligheid en risicobeoordeling vervult ook de volgende taken:

a) het is het contactpunt voor de veiligheidsinstanties van de andere instellingen van de Unie en voor de nationale veiligheidsinstanties bij kwesties in verband met de veiligheidsmachtigingsprocedures voor leden van het Europees Parlement, ambtenaren van het Europees Parlement en andere parlementaire medewerkers die in dienst van een fractie zijn;

b) het geeft de nodige algemene veiligheidsbriefing over de verplichting om gerubriceerde informatie te beschermen en de gevolgen van niet-nakoming van die verplichting;

c) het houdt toezicht op het fungeren van de beveiligde zone en de beveiligde leeskamers in de gebouwen van het Parlement, zo nodig in samenwerking met de veiligheidsdiensten van andere instellingen de Unie en van de NSA's;

d) het controleert, in samenwerking met de veiligheidsinstanties van andere instellingen van de Unie en de NSA's, de procedures voor het beheer en de opslag van gerubriceerde informatie, de beveiligde zone en de beveiligde leeskamers in de gebouwen van het Parlement waar gerubriceerde informatie wordt verwerkt;

e) het stelt de passende instructies voor behandeling voor aan de secretaris-generaal;

4.2. Het DIT is verantwoordelijk voor de verwerking bij het Europees Parlement van vertrouwelijke informatie met beveiligde IT-systemen.

4.3. De CIU is verantwoordelijk voor:

a) het identificeren van de beveiligingsbehoeften voor de doeltreffende bescherming van vertrouwelijke informatie, in nauwe samenwerking met het Directoraat Veiligheid en risicobeoordeling en het DIT en met de veiligheidsinstanties van de andere instellingen van de Unie;

b) het identificeren van alle aspecten van het beheer en de opslag van vertrouwelijke informatie binnen het Parlement, zoals vastgesteld in de instructies voor behandeling;

c) de werking van de beveiligde zone;

d) het beheer of de raadpleging van vertrouwelijke informatie in de beveiligde zone of in de beveiligde leeskamer van de CIU overeenkomstig artikel 7, leden 2 en 3, van dit besluit;

e) het beheer van het register van de CIU;

f) het rapporteren bij de veiligheidsinstantie van bewezen of vermoedelijke veiligheidsinbreuken of verlies of compromittering van vertrouwelijke informatie die bij de CIU is gedeponeerd en in de beveiligde zone of in de beveiligde leeskamer van de CIU wordt bewaard.

5. Voorts stelt de secretaris-generaal in zijn hoedanigheid van veiligheidsinstantie de volgende instanties aan:

a) een instantie voor beveiligingshomologatie (SAA);

b) een operationele instantie voor IA (IAOA);

c) een instantie voor cryptodistributie (CDA);

d) een Tempest-instantie (TA);

e) een instantie voor IA (IAA).

De uitoefening van die functies vereist geen afzonderlijke organisatorische entiteiten. Zij hebben afzonderlijke mandaten. Deze functies en de ermee samengaande verantwoordelijkheden kunnen echter in één organisatorische entiteit worden ondergebracht of geïntegreerd dan wel in meerdere organisatorische entiteiten worden gesplitst, mits belangenconflicten en dubbel werk worden voorkomen.

6. De SAA brengt over alle beveiligingskwesties met betrekking tot de homologatie van elk IT-systeem en -netwerk in het Parlement advies uit door:

6.1. erop toe te zien dat de CIS het toepasselijke beveiligingsbeleid en de beveiligingsrichtlijnen naleven, door het afgeven van een goedkeuringsverklaring voor de behandeling van gerubriceerde informatie door de CIS tot een bepaald rubriceringniveau in zijn operationele omgeving, met de voorwaarden voor de homologatie, en de criteria volgens welke hergoedkeuring nodig is;

6.2. een procedure voor veiligheidshomologatie vast te stellen overeenkomstig het desbetreffende beleid, met duidelijke goedkeuringsvoorwaarden voor de CIS die onder haar gezag staan;

6.3. een strategie voor veiligheidshomologatie op te stellen waarin de mate van gedetailleerdheid voor de homologatie wordt aangegeven, afhankelijk van het vereiste niveau van „assurance";

6.4. documentatie over beveiliging te bestuderen en goed te keuren, inclusief risicobeheer en verklaringen over resterende risico's, documenten ter staving van de beveiligingsimplementatie en operationele beveiligingsprocedures, en ervoor te zorgen dat die documentatie strookt met de regels en het beleid van het Parlement inzake beveiliging;

6.5. de implementatie van beveiligingsmaatregelen met betrekking tot de CIS te controleren door beveiligingsbeoordelingen, -inspecties of -toetsingen uit te voeren of te steunen;

6.6. beveiligingseisen (bijvoorbeeld machtigingsgraad van het personeel) voor gevoelige posten in verband met de CIS vast te stellen;

6.7. de interconnectie van een bepaald CIS met andere CIS goed te keuren of deel te nemen aan de gezamenlijke goedkeuring daarvan;

6.8. de beveiligingsnormen van overwogen technische apparatuur voor de veilige behandeling en de bescherming van gerubriceerde informatie goed te keuren;

6.9. erop toe te zien dat de encryptieproducten die bij het Europees Parlement worden gebruikt, op de lijst van door de Unie goedgekeurde producten staan; en

6.10. met de provider van het systeem, de beveiligingsmedewerkers en vertegenwoordigers van de gebruikers overleg te plegen over veiligheidsrisicobeheer, in het bijzonder het resterende risico, en de voorwaarden voor de goedkeuringsverklaring.

7. De IAOA is verantwoordelijk voor:

7.1. het ontwikkelen van beveiligingsdocumentatie die strookt met het beveiligingsbeleid en de beveiligingsrichtlijnen, waaronder met name de verklaring inzake het resterend risico, de operationele beveiligingsprocedures en het encryptieplan in de CIS-homologatieprocedure;

7.2. het deelnemen 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 toepasselijke beveiligingsdocumentatie;

7.3. het toezien op de uitvoering en toepassing van de operationele beveiligingsprocedures en, in voorkomend geval, het overdragen van operationele verantwoordelijkheden voor beveiliging aan de eigenaar van het systeem, namelijk de CIU;

7.4. het beheer van en het werken met encryptieproducten, de bewaring van versleutelde en gecontroleerde informatie en, indien nodig, het genereren van cryptografische variabelen;

7.5. het uitvoeren van evaluaties en tests van veiligheidsanalysen, in het bijzonder teneinde de door de SAA verlangde risicoverslagen op te stellen;

7.6. het aanbieden van CIS-specifieke opleidingen over IA;

7.7. het implementeren en toepassen van CIS-specifieke beveiligingsmaatregelen.

8. De CDA is verantwoordelijk voor:

8.1. het beheer van en de verantwoording voor encryptiemateriaal van de EU;

8.2. het toezicht, in nauwe samenwerking met de SAA, op de naleving van passende procedures en de opstelling van plannen voor verslaglegging over en veilige behandeling, opslag en verspreiding van al het encryptiemateriaal van de EU; en

8.3. de overdracht van encryptiemateriaal van de EU aan of van personen of diensten die er gebruik van maken.

9. De TA ziet erop toe dat de CIS het beleid en de instructies voor behandeling van Tempest in acht nemen. Zij keurt tegenmaatregelen van Tempest voor installaties en producten goed voor de bescherming van gerubriceerde informatie tot een bepaald rubriceringniveau in haar operationele omgeving.

10. De IAA is verantwoordelijk voor alle aspecten van het beheer en de behandeling van vertrouwelijke informatie in het Parlement en met name voor:

10.1 het ontwikkelen van beveiliging en beveiligingsrichtlijnen inzake IA en het toezien op de doeltreffendheid en pertinentie ervan;

10.2. het beschermen en beheren van technische informatie over encryptieproducten;

10.3. het garanderen dat de maatregelen inzake IA die zijn geselecteerd voor de bescherming van gerubriceerde informatie, voldoen aan het beleid inzake de geschiktheid en selectie van die maatregelen;

10.4. het garanderen dat encryptieproducten worden geselecteerd overeenkomstig het beleid inzake de geschiktheid en selectie ervan;

10.5. het overleg met de provider van het systeem, de beveiligingsmedewerkers en de vertegenwoordigers van gebruikers over beveiliging inzake IA.

**VEILIGHEIDSMEDEDELING 2**

BEHEER VAN GERUBRICEERDE INFORMATIE

A. **INLEIDING**

1. Deze veiligheidsmededeling bevat de voorschriften voor het beheer van vertrouwelijke informatie door het Parlement.

2. Wanneer hij vertrouwelijke informatie genereert, beoordeelt de opsteller het vertrouwelijkheidsniveau en beslist hij op basis van de in deze veiligheidsmededeling vermelde beginselen over de rubricering of markering van die informatie.

B. **EUCI-RUBRICERING**

3. Het besluit om een document te rubriceren, moet worden genomen voordat het document wordt opgesteld. Als informatie als EUCI wordt gerubriceerd, houdt dit in dat vooraf is beoordeeld hoe vertrouwelijk deze is en dat de opsteller ervan heeft besloten dat de ongeoorloofde openbaarmaking van deze informatie de belangen van de Europese Unie of van een of meer lidstaten of personen in meerdere of mindere mate zou kunnen schaden.

4. Als eenmaal is besloten de informatie te rubriceren, volgt een tweede beoordeling om het passende rubriceringsniveau te bepalen. Het rubriceringsniveau van een document wordt bepaald naar gelang van het niveau van gevoeligheid van de inhoud.

5. De verantwoordelijkheid voor het rubriceren van informatie berust uitsluitend bij de opsteller. Ambtenaren van het Parlement rubriceren informatie op instructie van of volgens een delegatie van de secretaris-generaal.

6. Met rubricering moet op een correcte en zuinige wijze worden omgesprongen. De opsteller van een te rubriceren document moet weerstand bieden aan elke neiging om het document te hoog of te laag te rubriceren.

7. Het rubriceringsniveau dat de informatie krijgt, bepaalt de mate van bescherming die eraan wordt verleend op het vlak van persoonsgerelateerde beveiliging, fysieke beveiliging, procedurele beveiliging en IA.

8. Informatie die aanleiding geeft tot rubricering moet als zodanig worden gemarkeerd en verwerkt, ongeacht de fysieke vorm ervan. De rubricering ervan moet duidelijk aan de ontvangers kenbaar worden gemaakt, in de vorm van een rubriceringsmarkering (als de informatie in geschreven vorm wordt verstrekt, op papier of binnen een CIS) of een mededeling (als de informatie mondeling wordt verstrekt, tijdens een gesprek of een vergadering achter gesloten deuren). Gerubriceerd materiaal moet fysiek worden gemarkeerd zodat het rubriceringsniveau duidelijk zichtbaar is.

9. EUCI in elektronische vorm mag alleen binnen een geaccrediteerd CIS worden gecreëerd. De gerubriceerde informatie zelf alsmede de bestandsnaam en het opslagmedium (indien dit extern is, bijvoorbeeld cd-rom's of USB-sticks) moeten altijd een rubriceringsmarkering hebben die overeenkomt met het rubriceringsniveau ervan.

10. Informatie moet worden gerubriceerd zodra zij vorm krijgt. Persoonlijke aantekeningen, kladteksten of e-mails waarin informatie staat die aanleiding geeft tot rubricering moeten direct als EUCI worden gemarkeerd en worden geproduceerd en verwerkt overeenkomstig de fysieke en technische eisen van de instructies voor behandeling. Deze informatie kan later de vorm aannemen van een officieel document dat eveneens op passende wijze zal worden gemarkeerd en verwerkt. Het is mogelijk dat een officieel document tijdens het redactieproces opnieuw moet worden beoordeeld en, naarmate het evolueert, een hogere of lagere rubricering moet krijgen.

11. De opsteller kan besluiten een standaardrubriceringsniveau toe te kennen aan categorieën informatie die hij regelmatig genereert. De opsteller moet er echter wel voor zorgen dat hij daarbij niet stelselmatig afzonderlijke delen informatie te hoog of te laag rubriceert.

12. EUCI moet altijd een rubriceringsmarkering hebben die overeenkomt met het rubriceringsniveau ervan.

B.1. ***Rubriceringsniveaus***

13. Voor EUCI worden de volgende rubriceringen gehanteerd:

— „TRÈS SECRET UE/EU TOP SECRET", als gedefinieerd in artikel 2, onder d), van dit besluit, als de compromittering ervan waarschijnlijk:

a) een rechtstreekse bedreiging zou vormen voor de interne stabiliteit van de Unie of een of meer van haar lidstaten, derde staten of internationale organisaties;

b) uitzonderlijk ernstige schade zou toebrengen aan de betrekkingen met derde staten of internationale organisaties;

c) rechtstreeks zou leiden tot grote aantallen dodelijke slachtoffers;

d) uitzonderlijk ernstige schade zou toebrengen aan de operationele doeltreffendheid of veiligheid van het ingezette personeel van de lidstaten of van andere contribuenten of aan de continue doeltreffendheid van uiterst waardevolle veiligheids- of inlichtingenoperaties; of

e) voor langere termijn ernstige schade zou toebrengen aan de economie van de Unie of haar lidstaten;

— „SECRET UE/EU SECRET", als gedefinieerd in artikel 2, onder d), van dit besluit, als de compromittering ervan waarschijnlijk:

a) aanzienlijke internationale spanningen zou doen ontstaan;

b) ernstige schade zou toebrengen aan de betrekkingen met derde staten en internationale organisaties;

c) rechtstreeks levensgevaar of ernstige schade aan de openbare orde of de individuele veiligheid of vrijheid zou veroorzaken;

d) belangrijke handels- of beleidsonderhandelingen zou schaden, met aanzienlijke operationele problemen voor de Unie of de lidstaten als gevolg;

e) ernstige schade zou toebrengen aan de operationele veiligheid van de lidstaten of aan de doeltreffendheid van uiterst waardevolle veiligheids- of inlichtingenoperaties;

f) wezenlijke materiële schade zou berokkenen aan de financiële, monetaire, economische en handelsbelangen van de Unie of een lidstaat;

g) de financiële levensvatbaarheid van belangrijke organisaties of bedrijven wezenlijk zou ondermijnen; of

h) de ontwikkeling of werking van beleidsvormen van de Unie ernstig zou hinderen, met grote economische, handels- of financiële gevolgen;

— „CONFIDENTIEL UE/EU CONFIDENTIAL", als gedefinieerd in artikel 2, onder d), van dit besluit, als de compromittering ervan waarschijnlijk:

a) de diplomatieke betrekkingen aanzienlijke schade zou berokkenen, bv. wanneer dit tot officieel protest of andere sancties zou leiden;

b) een gevaar zou vormen voor de veiligheid of vrijheid van het individu;

c) de uitkomst van handels- of beleidsonderhandelingen ernstig in gevaar zou brengen, met operationele problemen voor de Unie of een of meer lidstaten als gevolg;

d) schade zou toebrengen aan de operationele veiligheid van een of meer lidstaten of aan de doeltreffendheid van veiligheids- of inlichtingenoperaties;

e) de financiële levensvatbaarheid van belangrijke organisaties of bedrijven wezenlijk zou ondermijnen;

f) het onderzoek naar misdrijven of terroristische activiteiten zou verhinderen of het begaan ervan zou vergemakkelijken;

g) wezenlijk zou indruisen tegen de financiële, monetaire, economische en handelsbelangen van de Unie of de lidstaten; of

h) de ontwikkeling of werking van beleidsvormen van de Unie ernstig zou hinderen, met grote economische, handels- of financiële gevolgen;

— „RESTREINT UE/EU RESTRICTED", als gedefinieerd in artikel 2, onder d), van dit besluit, als de compromittering ervan waarschijnlijk:

a) nadelig zou zijn voor de algemene belangen van de EU;

b) de diplomatieke betrekkingen nadelig zou beïnvloeden;

c) aanzienlijk leed zou berokkenen aan personen of bedrijven;

d) nadelig zou zijn voor de Unie of de lidstaten bij handels- of beleidsonderhandelingen;

e) het moeilijker zou maken de veiligheid in de Unie of de lidstaten effectief te handhaven;

f) de effectieve ontwikkeling of werking van beleid van de Unie zou hinderen;

g) het goede beheer van de Unie en haar operaties zou ondermijnen;

h) inbreuk zou maken op verbintenissen van het Parlement om de gerubriceerde status van door derde partijen verstrekte gegevens te handhaven;

i) inbreuk zou maken op statutaire beperkingen op de openbaarmaking van informatie;

j) tot financiële verliezen zou leiden of oneigenlijke winsten of voordelen in de hand zou werken voor personen of ondernemingen; of

k) het onderzoek naar misdrijven zou schaden of het begaan ervan zou vergemakkelijken.

B.2. ***Rubricering van compilaties, dekbladen en uittreksels***

14. De rubricering van een brief of nota die bijvoegsels bevat, is even hoog als die van het hoogst gerubriceerde bijvoegsel. De opsteller moet duidelijk aangeven welke rubricering op de brief of nota moet worden toegepast indien deze van de bijvoegsels wordt gescheiden. Als een nota of brief niet gerubriceerd hoeft te worden, wordt aan het einde ervan het volgende vermeld: „Indien deze nota/brief van de bijvoegsels gescheiden wordt, is hij niet gerubriceerd".

15. Indien mogelijk worden documenten of bestanden met verschillende rubriceringsniveaus dusdanig gestructureerd dat de onderdelen met een verschillend rubriceringsniveau gemakkelijk kunnen worden herkend en, indien nodig, worden afgescheiden. De rubricering die voor het gehele document of bestand geldt, is minstens van hetzelfde niveau als die van het hoogst gerubriceerde gedeelte ervan.

16. Afzonderlijke bladzijden, punten, afdelingen, bijlagen, aanhangsels, aanhechtsels en bijvoegsels van een bepaald document kunnen verschillende rubriceringen vereisen en moeten dienovereenkomstig gemarkeerd worden. In documenten die EUCI bevatten, mogen standaardafkortingen worden gebruikt ter aanduiding van het rubriceringsniveau van afdelingen of onderdelen van tekst van minder dan één bladzijde.

17. Wanneer informatie van diverse herkomst wordt verzameld, wordt voor het eindproduct in zijn geheel nagegaan welk rubriceringsniveau het moet krijgen, aangezien hiervoor een hogere rubricering vereist kan zijn dan voor de onderdelen ervan.

C. **ANDERE VERTROUWELIJKE INFORMATIE**

18. „Andere vertrouwelijke informatie" wordt gemarkeerd overeenkomstig punt E van deze veiligheidsmededeling en de instructies voor behandeling.

D. **HET GENEREREN VAN VERTROUWELIJKE INFORMATIE**

19. Alleen personen die daartoe krachtens dit besluit bevoegd zijn of die daartoe door de SA zijn gemachtigd, mogen vertrouwelijke informatie genereren.

20. Vertrouwelijke informatie mag niet in documentenbeheersystemen voor internet of intranet worden opgenomen.

D.1. ***Het genereren van EUCI***

21. Om EUCI te genereren die als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" is gerubriceerd, moet de betrokkene daartoe krachtens dit besluit bevoegd zijn of daartoe vooraf in het bezit zijn van een machtiging uit hoofde van artikel 4, lid 1, van dit besluit.

22. EUCI die als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" is gerubriceerd, mag alleen binnen de beveiligde zone worden gegenereerd.

23. Op het genereren van EUCI zijn de volgende regels van toepassing:

a) op elke bladzijde wordt duidelijk het toepasselijke rubriceringsniveau aangegeven;

b) elke bladzijde wordt genummerd, met vermelding van het totale aantal bladzijden;

c) het document wordt voorzien van een referentienummer op de eerste bladzijde en een vermelding van het onderwerp, dat op zich geen gerubriceerde informatie mag zijn, tenzij het als zodanig wordt aangehecht;

d) op de eerste bladzijde van het document wordt een datum vermeld;

e) de eerste bladzijde van een document dat als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" is gerubriceerd, bevat een lijst van alle bijlagen en bijvoegsels;

f) documenten die als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" zijn gerubriceerd, zijn op elke bladzijde van een exemplaarnummer voorzien indien zij in meerdere exemplaren moeten worden verspreid. Op de eerste bladzijde van elk exemplaar wordt ook het totale aantal exemplaren en bladzijden vermeld; en

g) als in het document wordt verwezen naar andere documenten die van andere instellingen van de Unie ontvangen gerubriceerde informatie bevatten, of als het gerubriceerde informatie bevat die uit dergelijke documenten afkomstig is, krijgt het hetzelfde rubriceringsniveau als die documenten en mag het zonder voorafgaande schriftelijke toestemming van de opsteller niet worden verspreid onder andere personen dan de personen die zijn vermeld in de distributielijst van het (de) oorspronkelijke document (documenten) dat (die) gerubriceerde informatie bevat(ten).

24. De opsteller behoudt de controle over de door hem gegenereerde EUCI. Hij moet vooraf om schriftelijke toestemming worden verzocht voordat EUCI:

a) een lagere rubricering krijgt of wordt gederubriceerd;

b) voor andere dan de door de opsteller vastgestelde doeleinden wordt gebruikt;

c) wordt bekendgemaakt aan een derde staat of internationale organisatie;

d) wordt bekendgemaakt aan een andere persoon, instelling, land of internationale organisatie dan de geadresseerden die van de opsteller toestemming hebben gekregen om de desbetreffende informatie te raadplegen;

e) wordt bekendgemaakt aan een contractant of mogelijke contractant in een derde staat;

f) wordt gekopieerd of vertaald, indien de informatie gerubriceerd is als „TRES SECRET UE/EU TOP SECRET";

g) wordt vernietigd.

D.2. ***Het genereren van andere vertrouwelijke informatie***

25. De secretaris-generaal kan in zijn hoedanigheid van veiligheidsinstantie beslissen om een bepaalde functie, dienst en/of persoon al dan niet te machtigen om „andere vertrouwelijke informatie" te genereren.

26. Op „andere vertrouwelijke informatie" wordt een van de in de instructies voor behandeling gedefinieerde markeringen aangebracht.

27. Op het genereren van „andere vertrouwelijke informatie" zijn de volgende regels van toepassing:

a) de markering wordt bovenaan de eerste bladzijde van het document aangebracht;

b) elke bladzijde wordt genummerd, met vermelding van het totale aantal bladzijden;

c) het document wordt voorzien van een referentienummer op de eerste bladzijde en een vermelding van het onderwerp;

d) op de eerste bladzijde van het document wordt een datum vermeld;

e) de laatste bladzijde van het document bevat een lijst van alle bijlagen en bijvoegsels.

28. Voor het genereren van „andere vertrouwelijke informatie" gelden specifieke regels en procedures die in de instructies voor behandeling zijn vastgesteld.

E. **BEVEILIGINGSINDICATOREN EN MARKERINGEN**

29. Beveiligingsindicatoren en markeringen in documenten zijn bedoeld om de informatiestroom in goede banen te leiden en de toegang tot vertrouwelijke informatie te beperken op basis van het „need to know"-beginsel.

30. Wanneer beveiligingsindicatoren en markeringen worden gebruikt of toegevoegd, moet erop worden gelet geen verwarring te creëren met de EUCI-rubricering, namelijk „RESTREINT UE/EU RESTRICTED", „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" en „TRES SECRET UE/EU TOP SECRET".

31. Specifieke regels voor het gebruik van beveiligingsindicatoren en markeringen, alsook de lijst van goedgekeurde beveiligingsmarkeringen van het Europees Parlement, worden vastgesteld in de instructies voor behandeling.

E.1. ***Beveiligingsindicatoren***

32. Beveiligingsindicatoren mogen alleen worden gebruikt in combinatie met een rubricering en mogen niet afzonderlijk in documenten worden aangebracht. Op EUCI kan een beveiligingsindicator worden toegepast om:

a) de geldigheidsduur van een rubricering te beperken (wat voor gerubriceerde informatie inhoudt dat zij automatisch lager wordt gerubriceerd of wordt gederubriceerd);

b) de verspreiding van de EUCI in kwestie te beperken;

c) een speciale regeling voor behandeling vast te stellen ter aanvulling van die op grond van het rubriceringsniveau.

33. De extra controles op de behandeling en opslag van documenten die EUCI bevatten, brengen voor alle betrokkenen extra lasten met zich. Om de daarmee samenhangende werklast zoveel mogelijk te beperken, is het good practice om bij het genereren van een dergelijk document een geldigheidsduur of tijdstip vast te stellen waarna de rubricering automatisch verstrijkt en de informatie in het document wordt gerubriceerd of wordt gederubriceerd.

34. Wanneer een document een specifiek werkgebied betreft en de verspreiding ervan moet worden beperkt en/of aan speciale regelingen voor behandeling moet worden onderworpen, kan daartoe een verklaring aan de rubricering worden toegevoegd zodat het doelpubliek duidelijk wordt.

E.2. ***Markeringen***

35. Markeringen zijn geen rubricering. Zij dienen slechts om concrete instructies voor de behandeling van een document te geven en mogen niet worden gebruikt om de inhoud van een dergelijk document te beschrijven.

36. Markeringen kunnen afzonderlijk in documenten worden aangebracht of in combinatie met een rubricering worden gebruikt.

37. In de regel worden markeringen gebruikt voor informatie die onder de in artikel 339 VWEU en artikel 17 van het Statuut bedoelde geheimhoudingsplicht valt of die om juridische redenen door het Parlement moet worden beschermd, maar die niet hoeft of kan worden gerubriceerd.

E.3. ***Gebruik van markeringen in het CIS***

38. De regels voor het gebruik van markeringen zijn ook van toepassing in het gehomologeerde CIS.

39. De SAA stelt specifieke regels vast voor het gebruik van markeringen in het gehomologeerde CIS.

F. **ONTVANGST VAN INFORMATIE**

40. Binnen het Parlement is alleen de CIU bevoegd om informatie die als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd, van derde partijen te ontvangen.

41. Zowel de CIU als het bevoegde parlementaire orgaan/de bevoegde parlementaire ambtsdrager kunnen verantwoordelijk zijn voor de ontvangst van informatie die als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau is gerubriceerd en „andere vertrouwelijke informatie" van derde partijen en voor de toepassing van de in deze veiligheidsmededeling vermelde beginselen.

G. **REGISTRATIE**

42. Registratie betekent de toepassing van procedures voor het optekenen van de levenscyclus van vertrouwelijke informatie, ook de verspreiding, raadpleging en vernietiging ervan.

43. Voor de toepassing van deze veiligheidsmededeling betekent logboek een register waarin met name de datum en het tijdstip worden genoteerd waarop vertrouwelijke informatie:

a) bij het bevoegde secretariaat van het parlementaire orgaan/de parlementaire ambtsdrager c.q. de CIU binnenkomt of buitengaat;

b) wordt ingekeken door of doorgezonden aan een persoon met een veiligheidsmachtiging; en

c) wordt vernietigd.

44. De opsteller van gerubriceerde informatie is verantwoordelijk voor het markeren van de initiële verklaring bij het genereren van een document die dergelijke informatie bevat. Die verklaring wordt aan de CIU meegedeeld wanneer het document wordt gegenereerd.

45. Informatie die als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd, mag alleen voor veiligheidsdoeleinden in een CIS worden geregistreerd. Informatie die als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau is gerubriceerd en „andere vertrouwelijke informatie" die van derde partijen is ontvangen, wordt door de dienst die verantwoordelijk is voor de officiële ontvangst van het document, d.w.z. hetzij de CIU, hetzij het secretariaat van het parlementaire orgaan/de parlementaire ambtsdrager, voor administratieve doeleinden geregistreerd. Binnen het Parlement geproduceerde „andere vertrouwelijke informatie" wordt voor administratieve doeleinden geregistreerd door de opsteller.

46. Informatie die als „CONFIDENTIEL UE/CONFIDENTIEL EU", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd, wordt met name geregistreerd wanneer deze:

a) wordt gegenereerd;

b) bij de CIU binnenkomt of buitengaat; en

c) in het CIS binnenkomt of buitengaat.

47. Informatie die als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau is gerubriceerd, wordt met name geregistreerd wanneer deze:

a) wordt gegenereerd;

b) bij het bevoegde secretariaat van het parlementaire orgaan/de parlementaire ambtsdrager c.q. de CIU binnenkomt of buitengaat; en

c) in een CIS binnenkomt of buitengaat.

48. De registratie van vertrouwelijke informatie kan hetzij op papier, hetzij in een elektronisch logboek/CIS geschieden.

49. In het geval van informatie die als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau is gerubriceerd en „andere vertrouwelijke informatie" wordt ten minste het volgende geregistreerd:

a) de datum en het tijdstip waarop deze bij het bevoegde secretariaat van het parlementaire orgaan/de parlementaire ambtsdrager c.q. de CIU binnenkomt of buitengaat;

b) de titel van het document, het rubriceringsniveau of de markering, de datum waarop de rubricering/markering verstrijkt en het eventuele referentienummer van het document.

50. In het geval van informatie die als „CONFIDENTIEL UE/CONFIDENTIEL EU", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd wordt ten minste het volgende geregistreerd:

a) de datum en het tijdstip waarop deze bij de CIU binnenkomt of buitengaat;

b) de titel van het document, het rubriceringsniveau of de markering, het eventuele referentienummer van het document en de datum waarop de rubricering/markering verstrijkt;

c) de gegevens van de opsteller;

d) een register van de identiteit van elke persoon die toegang tot het document heeft gekregen en van de datum waarop het document door die persoon is ingekeken;

e) een register van eventuele kopieën of vertalingen die van het document zijn gemaakt;

f) de datum en het tijdstip waarop eventuele kopieën of vertalingen van het document bij de CIU buitengaan of terugkomen, en gegevens over aan wie ze zijn toegezonden en wie ze heeft teruggezonden;

g) de datum en het tijdstip waarop het document wordt vernietigd en door wie, overeenkomstig de beveiligingsvoorschriften van het Parlement voor vernietiging; en

h) de lderubricering of lagere rubricering van het document.

51. Logboeken worden zo nodig gerubriceerd of gemarkeerd. Logboeken voor informatie die als „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd, moeten op hetzelfde niveau worden gerubriceerd.

52. Gerubriceerde informatie mag worden geregistreerd:

a) in één logboek; of

b) in afzonderlijke logboeken, naar gelang van het rubriceringsniveau, de status als binnenkomende of uitgaande informatie en de oorsprong of bestemming van de informatie.

53. Indien de informatie elektronisch wordt verwerkt binnen het CIS, mogen de registratieprocedures verlopen met de middelen binnen het CIS zelf die aan gelijkwaardige eisen als bovengenoemde eisen voldoen. Wanneer EUCI het CIS verlaat, is bovengenoemde registratieprocedure van toepassing.

54. Het CIS registreert alle gerubriceerde informatie die door het Parlement wordt vrijgegeven aan derden en van gerubriceerde informatie die van derden wordt ontvangen.

55. Als de registratie van informatie die als „CONFIDENTIEL UE/CONFIDENTIEL EU", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd, eenmaal is voltooid, controleert de CIU of de geadresseerde een geldige veiligheidsmachtiging heeft. Zo ja, wordt de geadresseerde door de CIU in kennis gesteld. Gerubriceerde informatie mag slechts worden geraadpleegd nadat het document die deze informatie bevat, is geregistreerd.

H. **VERSPREIDING**

56. De opsteller stelt de initiële verzendlijst op voor de EUCI die hij heeft gegenereerd.

57. Informatie die als „RESTREINT UE/EU RESTRICTED" is gerubriceerd en „andere vertrouwelijke informatie" die door het Parlement is gegenereerd, wordt binnen het Parlement verspreid door de opsteller, overeenkomstig de desbetreffende instructies voor behandeling en op basis van het „need to know"-beginsel. In het geval van als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" gerubriceerde informatie die binnen het Parlement is gegenereerd, wordt de verzendlijst (en eventuele nader instructies voor verspreiding) verstrekt aan de CIU, die voor het beheer ervan verantwoordelijk is.

58. Door het Parlement gegenereerde EUCI mag alleen door de CIU aan derden worden verzonden, op basis van het „need to know"-beginsel.

59. Vertrouwelijke informatie die wordt ontvangen door hetzij de CIU, hetzij een orgaan/ambtsdrager van het parlement die daarom heeft verzocht, wordt verspreid overeenkomstig de instructies die de opsteller ervan heeft gegeven.

I. **BEHANDELING, OPSLAG EN RAADPLEGING**

60. De behandeling, de opslag en de raadpleging van vertrouwelijke informatie geschieden overeenkomstig veiligheidsmededeling 4 en de instructies voor behandeling.

J. **KOPIËREN/VERTALEN/VERTOLKEN VAN GERUBRICEERDE INFORMATIE**

61. Documenten die informatie bevatten die als „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd, mogen niet zonder voorafgaande schriftelijke toestemming van de opsteller worden gekopieerd of vertaald. Documenten die informatie bevatten die als „SECRET UE/EU SECRET" of op een gelijkwaardig niveau of „CONFIDENTIEL UE/EU CONFIDENTIAL" of op een gelijkwaardig niveau is gerubriceerd, mogen op instructie van de houder worden gekopieerd of vertaald, mits de opsteller dat niet heeft verboden.

62. Elke kopie van een document dat informatie bevat die als „TRES SECRET UE/EU TOP SECRET", „SECRET UE/EU SECRET" of „CONFIDENTIEL UE/EU CONFIDENTIAL"of op een gelijkwaardig niveau is gerubriceerd, wordt voor veiligheidsdoeleinden geregistreerd.

63. De beveiligingsmaatregelen die voor het originele document met gerubriceerde informatie gelden, zijn ook van toepassing op de kopieën en vertalingen ervan.

64. Documenten die van de Raad worden ontvangen, dienen in alle officiële talen te worden ontvangen.

65. Om kopieën en/of vertalingen van documenten die gerubriceerde informatie bevatten, mag door de opsteller of de houder van een kopie worden verzocht. Kopieën van documenten die informatie bevatten die als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau zijn gerubriceerd, mogen alleen in de beveiligde zone worden gemaakt, en wel op kopieerapparaten die deel uitmaken van een gehomologeerd CIS. Kopieën van documenten die informatie bevatten die als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau zijn gerubriceerd, moeten binnen de gebouwen van het Parlement worden gemaakt met gehomologeerde kopieerapparatuur.

66. Alle kopieën en vertalingen van een document of delen of kopieën van documenten die vertrouwelijke informatie bevatten, worden naar behoren gemarkeerd, genummerd en geregistreerd.

67. Er worden niet meer kopieën gemaakt dan strikt nodig is. Na afloop van de raadplegingstermijn moeten alle kopieën overeenkomstig de instructies voor behandeling worden vernietigd.

68. Alleen tolken en vertalers die ambtenaren van het Parlement zijn, krijgen toegang tot gerubriceerde informatie.

69. Tolken en vertalers die toegang hebben tot documenten die informatie bevatten die als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd, moeten de nodige veiligheidsmachtiging hebben.

70. Wanneer tolken en vertalers aan documenten werken die informatie bevatten die als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd, moeten zij in de beveiligde zone werken.

K. **LAGER RUBRICEREN, DERUBRICEREN EN DEMARKEREN VAN VERTROUWELIJKE INFORMATIE**

K.1. ***Algemene beginselen***

71. Vertrouwelijke informatie wordt gederubriceerd, lager gerubriceerd of gedemarkeerd wanneer de bescherming niet langer noodzakelijk is of niet langer op het oorspronkelijke niveau noodzakelijk is.

72. Besluiten om de informatie in binnen het Parlement gegenereerde documenten lager te rubriceren, te derubriceren of te demarkeren kunnen ook ad hoc worden genomen, bijvoorbeeld na een verzoek om inzage van het publiek of een andere instelling van de Unie of op initiatief van de CIU of het parlementaire orgaan/de parlementaire ambtsdrager.

73. Bij het genereren geeft de opsteller waar mogelijk aan of de EUCI op een bepaalde datum of na een bepaalde gebeurtenis lager gerubriceerd of gederubriceerd mag worden. Als het niet mogelijk is dat aan te geven, heroverwegen de opsteller, de CIU of het parlementaire orgaan dat/de parlementaire ambtsdrager die houder is van de informatie, het rubriceringsniveau van de EUCI ten minste om de vijf jaar. In elk geval mag EUCI alleen met voorafgaande schriftelijke toestemming van de opsteller lager gerubriceerd of gederubriceerd worden.

74. Indien de opsteller van EUCI niet kan worden vastgesteld of getraceerd, heroverweegt de veiligheidsinstantie de rubricering van de EUCI in kwestie op basis van een voorstel van het parlementaire orgaan dat/de parlementaire ambtsdrager die de informatie bewaart, die daartoe de CIU kan raadplegen.

75. De CIU of het parlementaire orgaan dat/de parlementaire ambtsdrager die houder is van de informatie, is verantwoordelijk voor het inlichten van de geadresseerden over de derubricering of lagere rubricering van de informatie, en die geadresseerden zijn op hun beurt verantwoordelijk voor het inlichten van eventuele verdere geadresseerden aan wie zij het document of een kopie daarvan hebben toegezonden.

76. De derubricering, lagere rubricering of demarkering van informatie in een document wordt geregistreerd.

K.2. ***Derubricering***

77. EUCI kan geheel of gedeeltelijk worden gederubriceerd. EUCI kan gedeeltelijk worden gederubriceerd wanneer bescherming niet langer nodig wordt geacht voor een bepaal deel van het document, maar gerechtvaardigd blijft voor de rest van het document.

78. Wanneer de heroverweging van EUCI in een binnen het Parlement gegenereerd document resulteert in een besluit tot derubricering, moet worden overwogen of het document openbaar mag worden gemaakt, dan wel een verspreidingsmarkering moet krijgen (d.w.z. niet openbaar mag worden gemaakt).

79. Wanneer EUCI wordt gederubriceerd, wordt de derubricering in het logboek geregistreerd met de volgende gegevens: datum van de derubricering, namen van de personen die om de derubricering hebben verzocht en daartoe toestemming hebben gegeven, referentienummer van het gederubriceerde document en uiteindelijke bestemming ervan.

80. De oude rubriceringsmarkeringen in het gederubriceerde document en in alle kopieën daarvan worden doorstreept. De documenten en alle kopieën daarvan worden dienovereenkomstig opgeslagen.

81. Na gedeeltelijke derubricering van gerubriceerde documenten wordt het gederubriceerde deel in de vorm van een uittreksel gegenereerd en dienovereenkomstig opgeslagen. De bevoegde dienst registreert:

a) de datum van de gedeeltelijke derubricering;

b) de namen van de personen die om de derubricering hebben verzocht en daartoe toestemming hebben gegeven; en

c) het referentienummer van het gederubriceerde uittreksel.

K.3. ***Lagere rubricering***

82. Nadat gerubriceerde informatie een lagere rubricering heeft gekregen, wordt het desbetreffende document in de logboeken voor zowel het oude als het nieuwe rubriceringsniveau geregistreerd. De datum van de lagere rubricering alsook de naam van de persoon die daarom heeft verzocht, worden geregistreerd.

83. Het document dat de lager gerubriceerde informatie bevat en alle kopieën daarvan krijgen het nieuwe rubriceringsniveau en worden dienovereenkomstig opgeslagen.

L. **VERNIETIGING VAN VERTROUWELIJKE INFORMATIE**

84. Vertrouwelijke informatie (papieren of elektronische versie) die niet langer nodig is, wordt vernietigd of gewist overeenkomstig de instructies voor behandeling en de desbetreffende archiveringsvoorschriften.

85. Informatie die als „TRES SECRET UE/EU TOP SECRET" of of „SECRET UE/EU SECRET" of op een gelijkwaardig niveau is gerubriceerd, wordt door de CIU vernietigd in aanwezigheid van een getuige die een veiligheidsmachtiging heeft voor ten minste het rubriceringsniveau van de te vernietigen informatie.

86. Informatie die als „TRES SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd, mag alleen met voorafgaande schriftelijke toestemming van de opsteller worden vernietigd.

87. Informatie die als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd, wordt door de CIU vernietigd en verwijderd op instructie van de opsteller of een bevoegde instantie. De logboeken en andere registers worden dienovereenkomstig geactualiseerd. Informatie die als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau is gerubriceerd, wordt hetzij door de CIU, hetzij door de het parlementaire orgaan/de parlementaire ambtsdrager vernietigd en verwijderd.

88. De ambtenaar die verantwoordelijk is voor de vernietiging en de getuige van de vernietiging ondertekenen een vernietigingscertificaat, dat door de CIU wordt bewaard en gearchiveerd. De CIU houdt, samen met de verspreidingsformulieren, de vernietigingscertificaten betreffende informatie die als „TRES SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd, gedurende ten minste tien jaar bij, en in het geval van informatie die als „SECRET UE/EU SECRET" of op een gelijkwaardig niveau of „CONFIDENTIEL UE/EU CONFIDENTIAL" of op een gelijkwaardig niveau is gerubriceerd, gedurende ten minste vijf jaar.

89. Documenten die gerubriceerde informatie bevatten, worden vernietigd volgens methoden die aan de toepasselijke normen van de Unie of gelijkwaardige normen voldoen om te voorkomen dat zij geheel of gedeeltelijk worden gereconstrueerd.

90. Digitale opslagmedia die voor gerubriceerde informatie zijn gebruikt, worden vernietigd overeenkomstig de desbetreffende instructies voor behandeling.

91. De vernietiging van gerubriceerde informatie wordt in het logboek geregistreerd met de volgende gegevens:

a) datum en tijdstip van vernietiging;

b) naam van de ambtenaar die verantwoordelijk is voor de vernietiging;

c) identificatie van het vernietigde document of de vernietigde kopieën;

d) oorspronkelijke fysieke vorm van de vernietigde EUCI;

e) wijze van vernietiging; en

f) plaats van vernietiging.

M. **ARCHIVERING**

92. Gerubriceerde informatie, met inbegrip van begeleidende nota's of brieven, bijlagen, afgiftebewijzen en/of andere onderdelen van het dossier, wordt zes maanden na de laatste raadpleging en uiterlijk één jaar na de deponering ervan naar het beveiligde archief in de beveiligde zone overgebracht. Nadere regels voor de archivering van gerubriceerde informatie worden in de instructies voor behandeling vastgesteld.

93. Op „andere vertrouwelijke informatie" zijn de algemene regels betreffende documentbeheer van toepassing, onverminderd eventuele andere specifieke voorschriften betreffende de behandeling ervan.

**VEILIGHEIDSMEDEDELING 3**

DE VERWERKING VAN VERTROUWELIJKE INFORMATIE DOOR MIDDEL VAN GEAUTOMATISEERDE COMMUNICATIE- EN INFORMATIESYSTEMEN (CIS)

A. **DE BORGING VAN IN INFORMATIESYSTEMEN VERWERKTE GERUBRICEERDE GEGEVENS**

1. Informatieborging (hierna: „Information Assurance — IA") op het gebied van informatiesystemen is het vertrouwen dat die systemen de erin opgenomen informatie zullen beschermen en zullen functioneren zoals nodig en wanneer nodig, onder toezicht van legitieme gebruikers. Doeltreffende IA waarborgt passende niveaus van vertrouwelijkheid, integriteit, beschikbaarheid, onweerlegbaarheid en authenticiteit. IA is op een risicobeheerproces gebaseerd.

2. „Communicatie- en informatiesystemen" (CIS) voor het verwerken van gerubriceerde informatie zijn systemen waarmee informatie in elektronische vorm kan worden verwerkt. Een dergelijk informatiesysteem omvat alle functionele bestanddelen die voor het functioneren ervan vereist zijn, waaronder infrastructuur, organisatie, personeel en informatiebronnen.

3. CIS verwerken gerubriceerde informatie overeenkomstig het concept van IA.

4. CIS worden aan een homologatieprocedure onderworpen. Met de homologatie wordt beoogd de verzekering te verkrijgen dat alle toepasselijke beveiligingsmaatregelen zijn getroffen en dat het niveau van bescherming van de gerubriceerde informatie en van het CIS overeenkomstig deze veiligheidsmededeling voldoende wordt geacht. In de homologatieverklaring worden de maximaal toegelaten rubriceringsgraad van de informatie die door het CIS mag worden verwerkt en de voorwaarden daarvoor vastgesteld.

5. Onderstaande IA-eigenschappen en -concepten zijn essentieel voor de beveiliging en de correcte werking van operaties met CIS.

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

b) beschikbaarheid: op verzoek van een gemachtigde entiteit toegankelijk en bruikbaar zijn;

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

d) integriteit: de nauwkeurigheid en de volledigheid van de informatie en de functionele bestanddelen worden gewaarborgd.

e) onweerlegbaarheid: het vermogen om te bewijzen dat een actie of gebeurtenis heeft plaatsgevonden, zodat deze niet vervolgens kan worden ontkend.

B. **BEGINSELEN VAN INFORMATION ASSURANCE**

6. De onderstaande bepalingen vormen de basis voor de beveiliging van alle CIS die voor het verwerken van gerubriceerde informatie worden gebruikt. In de beveiligingsbeleidsmaatregelen en beveiligingsrichtlijnen inzake IA moeten uitgebreide voorschriften voor de uitvoering van deze bepalingen worden vastgelegd.

B.1. ***Beheer van beveiligingsrisico's***

7. Beheer van veiligheidsrisico's is een integraal onderdeel van het omschrijven, ontwikkelen, exploiteren en onderhouden van een CIS. Risicobeheer (beoordeling, behandeling, aanvaarding en communicatie) verloopt als een zich herhalend proces, gezamenlijk uitgevoerd door vertegenwoordigers van de eigenaren van systemen, projectautoriteiten, exploitanten en veiligheidsgoedkeuringsinstanties, zoals bedoeld in veiligheidsmededeling 1, met gebruikmaking van een risicobeoordelingsprocedure die zichzelf heeft bewezen en transparant en begrijpelijk is. De reikwijdte van het CIS en zijn functionele bestanddelen wordt aan het begin van de risicobeheerprocedure duidelijk afgebakend.

8. De bevoegde instanties, zoals omschreven in veiligheidsmededeling 1, bezien de mogelijke dreigingen voor CIS en zorgen voor bijgewerkte en nauwkeurige dreigingsbeoordelingen die weergeven hoe de operationele omgeving van dat moment is. Zij werken voortdurend hun kennis inzake kwetsbaarheden bij en herzien op gezette tijden de kwetsbaarheidsbeoordeling, met het oog op aanpassing aan de veranderende informatietechnologieomgeving (IT).

9. De behandeling van veiligheidsrisico's is erop gericht een reeks beveiligingsmaatregelen toe te passen die een bevredigend evenwicht oplevert tussen de verlangens van de gebruikers, de kosten en het resterende veiligheidsrisico.

10. Homologatie van een CIS houdt mede een formele verklaring betreffende het resterende risico in en aanvaarding van dat resterende risico door een verantwoordelijke autoriteit. De door de bevoegde SAA bepaalde specifieke eisen, reikwijdte en gedetailleerdheid voor de homologatie van een CIS stemmen overeen met het ingeschatte risico, rekening houdend met alle relevante factoren, waaronder het rubriceringsniveau van de in het CIS verwerkte gerubriceerde informatie.

B.2. ***Beveiliging gedurende de levenscyclus van het CIS***

11. Beveiliging is gedurende de gehele levenscyclus van het CIS — vanaf de ingebruikname tot de buitengebruikstelling — een vereiste.

12. De rol en interactie van iedere bij een CIS betrokken partij in verband met de beveiliging ervan wordt voor iedere fase van de levenscyclus vastgesteld.

13. CIS, inclusief de maatregelen voor de technische en niet-technische beveiliging ervan, worden tijdens de homologatieprocedure aan beveiligingstests onderworpen om ervoor te zorgen dat het passende niveau van IA wordt bereikt en om na te gaan of CIS, inclusief de maatregelen voor de technische en niet-technische beveiliging ervan, correct zijn geïmplementeerd, geïntegreerd en geconfigureerd.

14. Beveiligingsbeoordelingen, inspecties en evaluaties worden op gezette tijden verricht tijdens de werking en het onderhoud van een CIS en wanneer zich uitzonderlijke omstandigheden voordoen.

15. De beveiligingsdocumentatie voor een CIS evolueert gedurende de levenscyclus van dat CIS als een integrerend deel van het proces van wijzigingsbeheer.

16. De door een CIS uitgevoerde registratieprocedures worden indien nodig geverifieerd als onderdeel van de homologatieprocedure.

B.3. ***Optimale werkwijzen***

17. De IAA ontwikkelt optimale werkwijzen voor de bescherming van door een CIS verwerkte gerubriceerde informatie. Richtlijnen inzake optimale toepassing beschrijven technische, fysieke, organisatorische en procedurele beveiligingsmaatregelen voor CIS, waarvan is aangetoond dat zij doeltreffend zijn in het bestrijden van dreigingen en kwetsbaarheden.

18. De bescherming van door CIS verwerkte gerubriceerde informatie steunt op de lering die door de bij IA betrokken entiteiten is getrokken.

19. De verspreiding en de daaropvolgende toepassing van optimale werkwijzen dragen bij aan het bereiken van een zelfde niveau van IA voor de CIS waarin gerubriceerde informatie wordt verwerkt en die door het secretariaat van het Parlement worden gebruikt.

B.4. ***Grondige verdediging***

20. Om de risico's voor CIS tot een minimum te beperken, wordt een reeks technische en niet-technische beveiligingsmaatregelen genomen, in de vorm van meerdere verdedigingslagen. Die lagen omvatten:

a) afschrikking: beveiligingsmaatregelen die vijandelijke plannen om het CIS aan te vallen, moeten ontraden;

b) preventie: beveiligingsmaatregelen die een aanval op het CIS moeten verhinderen of tegenhouden;

c) detectie: beveiligingsmaatregelen die moeten ontdekken dat het CIS wordt aangevallen;

d) veerkracht: beveiligingsmaatregelen die het effect van een aanval tot een zo klein mogelijke reeks informatie of onderdelen van CIS moeten beperken en verdere schade moeten voorkomen; en

e) herstel: beveiligingsmaatregelen die weer tot een veilige situatie voor het CIS moeten leiden.

Aan de hand van een risicobeoordeling wordt bepaald hoe streng die beveiligingsmaatregelen moeten zijn.

21. De bevoegde instanties, zoals omschreven in veiligheidsmededeling 1, zorgen ervoor dat zij kunnen reageren op incidenten die de organisatorische grenzen kunnen overschrijden om de reacties te coördineren en informatie uit te wisselen over deze incidenten en de ermee verband houdende risico's (computernoodhulpvaardigheden).

B.5. ***Beginsel van „minimalist and least privilege"***

22. Ter vermijding van onnodige risico's worden uitsluitend de functies, apparaten en diensten geactiveerd die essentieel zijn voor het vervullen van de operationele eisen.

23. Gebruikers van een CIS en geautomatiseerde processen krijgen alleen de toegang, voorrechten of machtigingen die zij nodig hebben voor het uitvoeren van hun taken, zodat schade ten gevolge van ongelukken, vergissingen of ongeoorloofd gebruik van CIS-middelen beperkt blijft.

B.6. ***Besef van informatieborging***

24. De eerste verdedigingslaag voor de beveiliging van CIS bestaat uit bewustwording van de risico's en de beschikbare beveiligingsmaatregelen.

Vooral alle personeelsleden die betrokken zijn bij de levenscyclus van CIS, met inbegrip van de gebruikers, moeten inzien:

a) dat beveiligingsfouten ernstige schade kunnen berokkenen aan CIS die gerubriceerde informatie verwerken;

b) dat interconnectiviteit en onderlinge afhankelijkheid kunnen leiden tot schade voor anderen; en

c) dat zij individuele verantwoordelijkheid en aansprakelijkheid dragen voor de beveiliging van CIS overeenkomstig hun functies binnen de systemen en processen.

25. Al het betrokken personeel, met inbegrip van het hogere kader, leden van het Europees Parlement en CIS-gebruikers, moeten verplicht een IA-opleiding en -bewustwordingstraining volgen, zodat goed wordt begrepen waar de verantwoordelijkheden inzake beveiliging liggen.

B.7. ***Evaluatie en goedkeuring van IT-beveiligingsproducten***

26. CIS die informatie die als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardige is gerubriceerd verwerken, worden zodanig beschermd dat de gerubriceerde informatie niet kan worden gecompromitteerd door onopzettelijke elektromagnetische emissies (hierna: „Tempest-beveiligingsmaatregelen").

27. Wanneer gerubriceerde informatie door versleutelingsproducten wordt beschermd, worden deze producten door de SAA gecertificeerd als door de Unie goedgekeurde versleutelingsproducten.

28. Tijdens de overdracht van gerubriceerde informatie met elektronische middelen moeten door de Unie goedgekeurde versleutelingsproducten worden gebruikt. Niettegenstaande deze eis kunnen specifieke procedures of specifieke technische configuraties worden toegepast in noodgevallen als bepaald in de punten 41 t/m 44.

29. De vereiste graad van vertrouwen in de beveiligingsmaatregelen, gedefinieerd als een niveau van IA, wordt bepaald aan de hand van de resultaten van de risicobeheersprocedure en het beveiligingsbeleid en de beveiligingsrichtlijnen in kwestie.

30. Het niveau van IA wordt geverifieerd middels internationaal erkende of nationaal goedgekeurde processen en technologieën. Dit omvat in de eerste plaats evaluatie, controles en audits.

31. De SAA stelt beveiligingsrichtlijnen vast inzake de kwalificatie en goedkeuring van IT-beveiligingsproducten die geen versleutelingsproducten zijn.

B.8. ***Overdracht binnen de beveiligde zone***

32. Wanneer de overdracht van gerubriceerde informatie beperkt is tot de beveiligde zone kan, op basis van het resultaat van een risicobeheerprocedure en behoudens goedkeuring van de SAA, gebruik worden gemaakt van onversleutelde verspreiding of van versleuteling op een lager niveau.

B.9. ***Beveiligde interconnectie van CIS***

33. Onder een interconnectie wordt verstaan: een rechtstreekse koppeling van twee of meer IT-systemen, met als doel het uitwisselen van gegevens en andere bronnen van informatie, in één of meer richtingen.

34. Een CIS beschouwt ieder gekoppeld IT-systeem als niet-vertrouwd en activeert beschermende maatregelen om de uitwisseling van gerubriceerde informatie met andere CIS te controleren.

35. Alle interconnecties van CIS aan een ander IT-systeem voldoen aan onderstaande basisvereisten:

a) de zakelijke of operationele vereisten voor dergelijke interconnecties worden door de bevoegde autoriteiten vastgelegd en goedgekeurd;

b) de interconnectie in kwestie wordt aan een procedure inzake risicobeheersing en accreditatie onderworpen en behoeft de goedkeuring van de SAA;

c) de perimeters van CIS worden opgezet met voorzieningen om de grenzen te beschermen.

36. Er wordt geen interconnectie tot stand gebracht tussen een geaccrediteerd CIS en een onbeschermd of openbaar netwerk, behalve indien voor dat doel in het CIS goedgekeurde grensbeschermingsvoorzieningen tussen het CIS en het onbeschermde of openbare netwerk zijn geïnstalleerd. De beveiligingsmaatregelen voor dergelijke interconnecties worden getoetst door de bevoegde IAA en goedgekeurd door de bevoegde SAA.

37. Wanneer het onbeschermde of openbare netwerk alleen als drager wordt gebruikt en de gegevens versleuteld zijn met een overeenkomstig lid 27 gecertificeerd versleutelingsproduct van de Unie, wordt zo'n koppeling niet gezien als een interconnectie.

38. De rechtstreekse interconnectie of de interconnectie in cascade met een onbeschermd of openbaar netwerk, van een CIS dat gehomologeerd is voor het verwerken van informatie die als „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardige niveau, „SECRET UE/EU SECRET" of op een gelijkwaardige niveau is gerubriceerd, is verboden.

B.10. ***Digitale opslagmedia***

39. Digitale opslagmedia worden vernietigd volgens procedures die de bevoegde veiligheidsautoriteit heeft goedgekeurd.

40. Digitale opslagmedia worden overeenkomstig de instructies voor behandeling hergebruikt, van een lagere rubricering voorzien of gederubriceerd.

B.11. ***Noodgevallen***

41. De hieronder beschreven specifieke procedures mogen worden toegepast in noodgevallen, zoals dreigende of uitgebroken crises, conflicten, oorlogssituaties of in uitzonderlijke operationele omstandigheden.

42. Gerubriceerde informatie mag met toestemming van de bevoegde autoriteit door middel van voor een lager rubriceringsniveau goedgekeurde versleutelingsproducten of zonder versleuteling worden overgedragen, indien vertraging schade zou veroorzaken die duidelijk zwaarder weegt dan de schade ten gevolge van de verspreiding van het gerubriceerde materiaal en indien:

a) de zender en de ontvanger niet over de vereiste versleutelingsapparatuur beschikken of helemaal geen versleutelingsapparatuur hebben; en

b) het gerubriceerde materiaal niet op tijd met andere middelen kan worden verstuurd.

43. Gerubriceerde informatie die in de in punt 41 bedoelde omstandigheden wordt overgedragen, mag geen tekenen of aanwijzingen dragen die haar onderscheidt van ongerubriceerde informatie of van informatie die door een beschikbaar versleutelingsproduct kan worden beschermd. Ontvangers worden onverwijld langs andere wegen op de hoogte gebracht van het rubriceringsniveau.

44. Indien gebruik wordt gemaakt van punt 41 of punt 42, wordt nadien een verslag opgesteld voor de bevoegde instantie.

**VEILIGHEIDSMEDEDELING 4**

FYSIEKE BEVEILIGING

A. **INLEIDING**

Deze veiligheidsmededeling omvat de beveiligingsbeginselen voor het scheppen van een veilige omgeving voor het correct verwerken van gerubriceerde informatie binnen het Europees Parlement. Die beginselen, inclusief die betreffende de technische beveiliging, worden aangevuld met de instructies voor behandeling.

B. **BEHEER VAN BEVEILIGINGSRISICO'S**

1. Risico's voor gerubriceerde informatie worden beheerd als een proces. Dat proces is gericht op het bepalen van de bekende veiligheidsrisico's, het vaststellen van beveiligingsmaatregelen om deze risico's tot een aanvaardbaar niveau te beperken conform de grondbeginselen en minimumnormen van deze veiligheidsmededeling, en het toepassen van die maatregelen overeenkomstig het begrip „grondige verdediging", zoals omschreven in veiligheidsmededeling 3. De doeltreffendheid van deze maatregelen wordt constant geëvalueerd.

2. De beveiligingsmaatregelen ter bescherming van gerubriceerde informatie gedurende haar gehele levenscyclus zijn evenredig met, in het bijzonder, de rubricering, de vorm en de omvang van de informatie of het materiaal in kwestie, de locatie en constructie van faciliteiten waar de gerubriceerde informatie in is ondergebracht en de lokaal beoordeelde dreiging van kwaadwillige en/of criminele activiteiten, met inbegrip van spionage, sabotage en terrorisme.

3. In de rampenplannen wordt rekening gehouden met de noodzaak om gerubriceerde informatie in noodsituaties te beschermen, teneinde toegang en openbaarmaking zonder machtiging of aantasting van de integriteit of beschikbaarheid te voorkomen.

4. In de bedrijfscontinuïteitsplannen worden preventie- en herstelmaatregelen opgenomen om de gevolgen van ernstige storingen of incidenten voor de verwerking en opslag van gerubriceerde informatie zo gering mogelijk te houden.

C. **ALGEMENE BEGINSELEN**

5. De rubricerings- of markeringsgraad die aan de informatie wordt toegekend, bepaalt welk beschermingsniveau van toepassing is ten aanzien van de fysieke beveiliging ervan.

6. Informatie die aanleiding geeft tot rubricering moet als zodanig worden gemarkeerd en verwerkt, ongeacht de fysieke vorm ervan. De rubricering ervan wordt duidelijk aan de ontvangers kenbaar gemaakt, in de vorm van een rubriceringsmarkering (als de informatie schriftelijk wordt verstrekt, op papier of in het CIS) of een mededeling (als de informatie mondeling wordt verstrekt, bijvoorbeeld in een gesprek of tijdens een presentatie). Gerubriceerd materiaal wordt fysiek zodanig gemarkeerd dat de rubriceringsgraad duidelijk zichtbaar is.

7. Vertrouwelijke informatie wordt in geen enkel geval gelezen op openbare plaatsen waar zij kan worden gezien door personen die geen noodzaak tot kennisname („need to know") hebben, zoals treinen, vliegtuigen, cafés of bars. Zij wordt niet op hotelkamers of in hotelkluisjes achtergelaten. Zij wordt niet onbeheerd op openbare plaatsen achtergelaten.

D. **VERANTWOORDELIJKHEDEN**

8. De CIU is verantwoordelijk voor de waarborging van de fysieke beveiliging bij het beheren van vertrouwelijke informatie die in haar beveiligde ruimten is opgeslagen. Ook is de CIU verantwoordelijk voor het beheer van haar beveiligde ruimten.

9. De fysieke beveiliging bij het beheer van informatie die als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau is gerubriceerd, of van „andere vertrouwelijke informatie", is de verantwoordelijkheid van het bevoegde parlementaire orgaan/de bevoegde parlementaire ambtsdrager.

10. Het directoraat Veiligheid en risicobeoordeling draagt zorg voor de persoonlijke beveiliging en de veiligheidsmachtiging die noodzakelijk zijn voor de veilige verwerking van vertrouwelijke informatie binnen het Europees Parlement.

11. Het DIT brengt advies uit en ziet erop toe dat alle gecreëerde en gebruikte CIS volledig in overeenstemming zijn met veiligheidsmededeling 3 en de bijbehorende instructies voor behandeling.

E. **BEVEILIGDE RUIMTEN**

12. Beveiligde ruimten kunnen overeenkomstig de technische beveiligingsnormen worden geïnstalleerd, volgens de graad die aan de vertrouwelijke informatie is toegekend zoals omschreven in artikel 7.

13. De beveiligde ruimten worden door de SAA gecertificeerd en door de veiligheidsinstantie gevalideerd.

F. **RAADPLEGING VAN VERTROUWELIJKE INFORMATIE**

14. Wanneer als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau gerubriceerde informatie bij de CIU is gedeponeerd en buiten de beveiligde zone moet worden geraadpleegd, voorziet de CIU de passende bevoegde dienst van een kopie. De bevoegde dienst zorgt ervoor dat de raadpleging en behandeling van de informatie in kwestie in overeenstemming zijn met de artikelen 8, lid 2, en artikel 10 van dit besluit en de desbetreffende instructies voor behandeling.

15. Wanneer als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau gerubriceerde informatie of „andere vertrouwelijke informatie" is gedeponeerd bij een ander parlementair orgaan of een andere parlementaire ambtsdrager dan de CIU, ziet het secretariaat van het parlementair orgaan of de parlementaire ambtsdrager in kwestie erop toe dat de raadpleging en behandeling van de informatie in kwestie in overeenstemming zijn met artikel 7, lid 3, artikel 8, leden 1, 2, en 4, artikel 9, leden 3, 4, en 5, artikel 10, leden 2 t/m 6, en artikel 11 van dit besluit en de desbetreffende instructies voor behandeling.

16. Wanneer als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau gerubriceerde informatie buiten de beveiligde zone moet worden geraadpleegd, ziet de CIU erop toe dat de raadpleging en behandeling van de informatie in kwestie in overeenstemming zijn met de artikelen 9 en 10 van dit besluit en de desbetreffende instructies voor behandeling.

G. **TECHNISCHE BEVEILIGING**

17. Technische beveiligingsmaatregelen vallen onder de verantwoordelijkheid van de SAA, die in de desbetreffende instructies voor behandeling vaststelt welke specifieke technische beveiligingsmaatregelen moeten worden toegepast.

18. Beveiligde leeskamers voor de raadpleging van als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau gerubriceerde informatie dan wel „andere vertrouwelijke informatie" voldoen aan specifieke technische beveiligingsmaatregelen zoals omschreven in de instructies voor behandeling.

19. De beveiligde ruimte omvat de volgende voorzieningen:

a) een onderzoeksruimte voor gecontroleerde toegang die volgens de technische beveiligingsmaatregelen uit de instructies voor behandeling wordt geïnstalleerd. De toegang tot deze ruimte wordt geregistreerd. De onderzoeksruimte voldoet aan hoge normen voor de identificatie van personen die toegang wordt geboden, videoregistratie, veilige bewaarplaatsen voor persoonlijke bezittingen die verboden zijn binnen de beveiligde ruimten (telefoons, pennen enzovoorts);

b) een gespreksruimte voor de overdracht en ontvangst van gerubriceerde informatie, met inbegrip van versleutelde gerubriceerde informatie, in overeenstemming met veiligheidsmededeling 3 en de desbetreffende instructies voor behandeling;

c) een beveiligd archief, waar goedgekeurde en gecertificeerde opbergruimten afzonderlijk worden gebruikt voor informatie die als „RESTREINT UE/EU RESTRICTED", „CONFIDENTIEL UE/EU CONFIDENTIAL" of „SECRET EU/EU SECRET" of op een gelijkwaardig niveau is gerubriceerd. Informatie die als „TRES SECRET UE/EU TOP SECRET" of gelijkwaardig is gerubriceerd, wordt in een afzonderlijke ruimte in een specifieke gecertificeerde container bewaard. Het enige aanvullende beschikbare materiaal in deze ruimte is de helpdesk voor het beheren van het archief door de CIU;

d) een registratieruimte, die voorzien is van de nodige middelen voor een papieren of elektronische registratie en van de nodige beveiligde voorzieningen voor het installeren van de toepasselijke CIS. Alleen de registratieruimte mag goedgekeurde en gehomologeerde kopieerapparatuur bevatten (voor het maken van papieren of elektronische kopieën). In de instructies voor behandeling wordt vermeld welke kopieerapparatuur is goedgekeurd en gehomologeerd. De registratieruimte voorziet voorts in de noodzakelijke ruimte voor de opslag en verwerking van geaccrediteerd materiaal om gerubriceerde informatie in fysieke vorm te kunnen markeren, kopiëren en verzenden, per rubriceringsgraad. Al het geaccrediteerde materiaal wordt omschreven door de CIU en geaccrediteerd door de SAA, op advies van de IAOA. Deze ruimte is ook uitgerust met geaccrediteerde vernietigingsapparatuur die is goedgekeurd voor de hoogste rubriceringsgraad, zoals omschreven in de instructies voor behandeling. De vertaling van informatie die als „CONFIDENTIEL UE/EU CONFIDENTIAL EU", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd, vindt plaats in de registratieruimte, in het toepasselijke en geaccrediteerde systeem. De registratieruimte biedt werkplekken voor maximaal twee vertalers tegelijkertijd en voor hetzelfde document. Hierbij is één personeelslid van de CIU aanwezig.

e) een leeskamer, voor het individueel raadplegen van gerubriceerde informatie door naar behoren gemachtigde personen. De leeskamer biedt voldoende ruimte voor twee personen, met inbegrip van een personeelslid van de CIU, dat te allen tijde bij iedere raadpleging aanwezig is. Het beveiligingsniveau van deze kamer is ontworpen voor de raadpleging van informatie die als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd. De leeskamer kan worden uitgerust met Tempestapparatuur om waar nodig in elektronische raadpleging te voorzien, in overeenstemming met de rubriceringsgraad van de informatie.

f) een vergaderzaal, die voldoende plaats biedt aan 25 personen voor het bespreken van informatie die als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET EU/EU SECRET" of op een gelijkwaardig niveau is gerubriceerd. De vergaderzaal biedt de nodige beveiligde en gecertificeerde technische voorzieningen voor vertolking in en vanuit maximaal twee talen. Wanneer zij niet voor vergaderingen wordt gebruikt, kan de vergaderzaal ook dienst doen als aanvullende leesruimte voor individuele raadpleging. In uitzonderlijke gevallen kan de CIU meer dan één gemachtigde persoon toestaan gerubriceerde informatie te raadplegen, op voorwaarde dat de machtigingsgraad en de noodzaak tot kennisname voor alle personen in de ruimte gelijk is. Er mogen maximaal vier personen tegelijkertijd vertrouwelijke informatie raadplegen. De aanwezigheid van CIU-personeel wordt versterkt.

g) beveiligde technische ruimten voor het bewaren van alle technische apparatuur die verband houdt met de beveiliging van de beveiligde zones en de beveiligde IT-servers.

20. De beveiligde zone voldoet aan de toepasselijke internationale beveiligingsnormen en is gecertificeerd door het directoraat Veiligheid en risicobeoordeling. De beveiligde zone voorziet in de volgende minimumvoorschriften met betrekking tot beveiliging en techniek:

a) alarm- en bewakingssystemen;

b) veiligheidsapparatuur- en noodsystemen (waarschuwingssysteem in twee richtingen);

c) een gesloten tv-circuit;

d) indringerdetectiesystemen;

e) toegangscontrole (met inbegrip van een biometrisch beveiligingssysteem);

f) containers;

g) kluisjes;

h) anti-elektromagnetische bescherming.

21. Indien aanvullende technische beveiligingsmaatregelen nodig zijn, kunnen zij worden toegevoegd door de SAA, in nauwe samenwerking met de CIU en na goedkeuring van de veiligheidsinstantie.

22. De infrastructuurapparatuur kan worden gekoppeld aan de algemene beheerssystemen van het gebouw waarin de beveiligde zone zich bevindt. De beveiligingsapparatuur voor toegangscontrole en voor de CIS blijven echter los staan van alle andere soortgelijke apparatuur binnen het Europees Parlement.

## H. **INSPECTIE VAN DE BEVEILIGDE ZONE**

23. De SAA voert regelmatig en op verzoek van de CIU inspecties van de beveiligde zone uit.

24. De SAA stelt, in overeenstemming met de instructies voor behandeling, een controlelijst voor beveiligingsinspecties op met de punten die tijdens een inspectie moeten worden geverifieerd, en houdt deze lijst bij.

## I. **VERVOER VAN VERTROUWELIJKE INFORMATIE**

25. Vertrouwelijke informatie wordt uit het zicht vervoerd, zonder enige indicatie over de vertrouwelijke aard van de inhoud ervan, in overeenstemming met de instructies voor behandeling.

26. Alleen bodes of personeel met de passende veiligheidsmachtiging mogen informatie bij zich dragen die als „CONFIDENTIEL UE/CONFIDENTIEL EU", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd.

27. Vervoer van vertrouwelijke infpormatie per externe post of met de hand buiten een gebouw gebeurt altijd in overeenstemming met de voorwaarden die zijn vastgelegd in de instructies voor behandeling.

28. Informatie die als „CONFIDENTIEL UE/CONFIDENTIEL EU", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd, wordt nooit per e-mail of fax verstuurd, zelfs niet wanneer er een beveiligd e-mailsysteem of cryptofax is geïnstalleerd. Informatie die als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau is gerubriceerd mag, evenals andere vertrouwelijke informatie, via e-mail worden verzonden indien een geaccrediteerd versleutelingssysteem wordt gebruikt.

## J. **OPSLAG VAN VERTROUWELIJKE INFORMATIE**

29. De rubricerings- of markeringsgraad die aan de informatie wordt toegekend, bepaalt welk beschermingsniveau van toepassing is ten aanzien van de opslag ervan. De informatie wordt opgeslagen in voor deze doelstelling gecertificeerde apparatuur, in overeenstemming met de instructies voor behandeling.

30. Informatie die als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau is gerubriceerd en „andere vertrouwelijke informatie" wordt:

a) wanneer zij niet wordt gebruikt opgeslagen in een reglementaire, stalen, vergrendelde kast, binnen een kantoor of een werkplek;

b) niet onbeheerd achtergelaten, tenzij zij naar behoren is opgeborgen en vergrendeld;

c) niet achtergelaten op een bureau, tafel enzovoorts op een manier dat niet-gemachtigde personen, zoals bezoekers en schoonmaak- of onderhoudspersoneel, de informatie kunnen lezen of meenemen;

d) niet getoond aan of besproken met niet-gemachtigde personen.

31. Informatie die als „RESTREINT UE/EU RESTRICTED" of op een gelijkwaardig niveau is gerubriceerd, en „andere vertrouwelijke informatie", wordt overeenkomstig de instructies voor behandeling enkel opgeslagen binnen het secretariaat van het parlementaire orgaan/de parlementaire ambtsdrager, of binnen de CIU;

32. Informatie die als „CONFIDENTIEL UE/CONFIDENTIEL EU", „SECRET UE/EU SECRET" of „TRÈS SECRET UE/EU TOP SECRET" of op een gelijkwaardig niveau is gerubriceerd, wordt:

a) in een beveiligde zone opgeslagen in een beveiligde container of in een kluis. Bij wijze van uitzondering, bijvoorbeeld als de CIU gesloten is, mag de informatie worden opgeslagen in een goedgekeurde en gecertificeerde kluis binnen de veiligheidsdiensten;

b) op geen enkel moment onbeheerd binnen de beveiligde zone achtergelaten, zonder dat zij eerst in een goedgekeurde kluis is opgeborgen (zelfs voor een zeer korte afwezigheid);

c) niet achtergelaten op een bureau, tafel enzovoorts op dusdanige wijze dat niet-gemachtigde personen de informatie kunnen lezen of meenemen, zelfs wanneer het bevoegde personeelslid van de CIU in de ruimte blijft.

Wanneer binnen de beveiligde zone een document met gerubriceerde informatie in elektronische vorm wordt opgesteld, wordt de computer vergrendeld en het scherm ontoegankelijk gemaakt zodra de schrijver van het document of het bevoegde personeelslid van de CIU de ruimte verlaat (zelfs voor een zeer korte afwezigheid). Een automatisch veiligheidsslot dat na enkele minuten wordt geactiveerd, is geen toereikende maatregel.

**VEILIGHEIDSMEDEDELING 5**

INDUSTRIËLE BEVEILIGING

A. **INLEIDING**

1. Deze veiligheidsmededeling heeft enkel betrekking op vertrouwelijke informatie.

2. Zij bevat bepalingen voor de toepassing van de gemeenschappelijke minimumnormen van bijlage I, deel 1, van dit besluit.

3. Industriële veiligheid is de toepassing van maatregelen om de bescherming van gerubriceerde informatie door contractanten of subcontractanten tijdens precontractuele onderhandelingen en tijdens de volledige looptijd van gerubriceerde opdrachten te waarborgen. In het kader van dergelijke opdrachten mag geen toegang worden verleend tot informatie met de rubricering „TRÈS SECRET UE/EU TOP SECRET".

4. Het Europees Parlement zorgt er als aanbestedende instantie voor dat aan de in dit besluit en in de gerubriceerde opdrachten vervatte minimumnormen voor industriële veiligheid is voldaan bij het plaatsen van gerubriceerde opdrachten bij industriële of andere entiteiten.

B. **BEVEILIGINGSELEMENTEN IN EEN GERUBRICEERDE OPDRACHT**

B.1. ***Gids voor beveiligingsrubricering (GBR)***

5. Alvorens een aanbesteding uit te schrijven of een gerubriceerde opdracht te gunnen, bepaalt het Europees Parlement als aanbestedende instantie welke rubricering wordt gegeven aan gegevens die aan inschrijvers en contractanten moeten worden verstrekt, en welke rubricering wordt gegeven aan gegevens die de contractant zal genereren. Voor dat doel stelt het een gids voor beveiligingsrubricering (GBR) op die bij de uitvoering van de opdracht moet worden gebruikt.

6. Voor het bepalen van de rubriceringsgraad van de diverse onderdelen van een gerubriceerde opdracht gelden onderstaande beginselen:

a) bij het opstellen van een GBR houdt het Europees Parlement rekening met alle ter zake doende beveiligingsaspecten, zoals de rubricering die is gegeven aan informatie die is verstrekt en goedgekeurd door de opsteller van de informatie voor gebruik met betrekking tot de opdracht;

b) de algehele rubriceringsgraad van de opdracht kan niet lager zijn dan de hoogste rubriceringsgraad van een van haar onderdelen.

B.2. ***Memorandum over de beveiligingsaspecten (MBA)***

7. De specifieke beveiligingseisen voor de opdracht worden beschreven in een memorandum over de beveiligingsaspecten (MBA). Het MBA bevat in voorkomend geval de GBR en maakt integraal deel uit van een gerubriceerde opdracht of opdracht in onderaanneming.

8. Het MBA bevat bepalingen die de contractant en/of de subcontractant verplichten zich te houden aan de minimumbeveiligingsnormen in dit besluit. Niet-naleving van deze minimumnormen kan voldoende reden zijn voor opzegging van de opdracht.

B.3. ***Programma-/projectbeveiligingsinstructies (PBI)***

9. Afhankelijk van het toepassingsgebied van programma's of projecten waarvoor toegang tot of verwerking of opslag van EUCI nodig is, kan de aanbestedende instantie die het programma of het project zal beheren, specifieke programma-/projectbeveiligingsinstructies (PBI) opstellen.

C. **VEILIGHEIDSMACHTIGING VOOR EEN VESTIGING (VMV)**

10. Een VMV wordt verleend door de nationale veiligheidsinstantie of een andere bevoegde instantie van een lidstaat en toont overeenkomstig de nationale wetten en regelgeving aan dat een industriële of andere entiteit binnen haar vestigingen in staat is gerubriceerde EUCI te beschermen die als „CONFIDENTIEL UE/EU CONFIDENTIAL" of „SECRET UE/EU SECRET" of op een gelijkwaardig niveau is gerubriceerd. Voordat aan een contractant of subcontractant of mogelijke contractant of subcontractant EUCI mag worden verstrekt of toegang tot EUCI mag worden verleend, wordt een bewijs van de VMV overgelegd aan het Europees Parlement, als aanbestedende instantie.

11. In het kader van een VMV wordt:

a) de integriteit van de industriële of andersoortige entiteit geëvalueerd;

b) de verantwoordelijkheid geëvalueerd, evenals de controle of de ontvankelijkheid voor ongewenste invloed, die als een veiligheidsrisico kan worden beschouwd;

c) nagegaan of de industriële of andere entiteit in de vestiging een beveiliging heeft geïnstalleerd die alle passende beveiligingsmaatregelen omvat die nodig zijn voor het beschermen van informatie of materiaal met rubriceringsniveau „CONFIDENTIEL UE/EU CONFIDENTIAL" of „SECRET UE/EU SECRET", overeenkomstig de in dit besluit vastgelegde vereisten;

d) nagegaan of de personeelsveiligheidsstatus van management, eigenaars en werknemers die toegang moeten hebben tot informatie met rubriceringsniveau „CONFIDENTIEL UE/EU CONFIDENTIAL" of „SECRET UE/EU SECRET", voldoet aan de in dit besluit vastgelegde vereisten;

e) nagegaan of de industriële of andere entiteit een vestigingsbeveiligingsfunctionaris heeft benoemd die tegenover het management verantwoordelijk is voor de handhaving van de veiligheidsverplichtingen in de entiteit.

12. In voorkomend geval deelt het Europees Parlement, als aanbestedende instantie, de nationale veiligheidsinstantie of een andere bevoegde veiligheidsinstantie mee dat in de precontractuele fase of voor de uitvoering van de opdracht een VMV vereist is. Een VMV of een persoonlijke veiligheidsmachtiging (PVM) wordt verlangd in de precontractuele fase waarin informatie met rubricering „CONFIDENTIEL UE/EU CONFIDENTIAL" of „SECRET UE/EU SECRET" moet worden verstrekt in het stadium van de offertes.

13. De aanbestedende instantie kent geen gerubriceerde opdracht toe aan een geselecteerde inschrijver zonder van de nationale veiligheidsinstantie of een andere bevoegde veiligheidsinstantie van de lidstaat waar de contractant of subcontractant is geregistreerd, een bevestiging te hebben ontvangen dat er, indien zulks vereist is, een VMV is afgegeven.

14. De bevoegde veiligheidsinstantie die een VMV heeft afgegeven brengt het Europees Parlement, de aanbestedende instantie, op de hoogte van wijzigingen die de VMV betreffen. Bij onderaanneming wordt de bevoegde veiligheidsinstantie op de hoogte gebracht.

15. Intrekking van een VMV door de nationale veiligheidsinstantie of een andere bevoegde veiligheidsinstantie biedt het Europees Parlement, de aanbestedende instantie, voldoende redenen om een gerubriceerde opdracht te beëindigen of een inschrijver uit te sluiten van mededinging.

D. **GERUBRICEERDE OPDRACHTEN EN ONDERAANNEMING**

16. Wanneer in de precontractuele fase gerubriceerde informatie wordt verstrekt aan een inschrijver, bevat de uitnodiging tot inschrijving een bepaling die de inschrijver die uiteindelijk geen offerte doet, of die niet wordt geselecteerd, verplicht alle gerubriceerde documenten binnen een bepaalde termijn terug te zenden.

17. Zodra een gerubriceerde opdracht of opdracht in onderaanneming is gegund, deelt het Europees Parlement, als aanbestedende instantie, de nationale veiligheidsinstantie van de contractant of subcontractant en/of een andere bevoegde veiligheidsinstantie de beveiligingsbepalingen van de gerubriceerde opdracht mee.

18. Na afloop van zulke opdrachten, deelt het Europees Parlement, als aanbestedende dienst (en/of, bij onderaanneming, de bevoegde veiligheidsinstantie, naargelang het geval) dit mee aan de nationale veiligheidsinstantie of een andere bevoegde veiligheidsinstantie van de lidstaat waar de contractant of subcontractant is geregistreerd.

19. Als algemene regel geldt dat de contractant of subcontractant alle gerubriceerde informatie die hij in zijn bezit heeft, na voltooiing van de gerubriceerde opdracht of onderaanneming moet terugbezorgen aan de aanbestedende instantie.

20. In het MBA worden specifieke bepalingen opgenomen voor het verwijderen van gerubriceerde informatie tijdens de uitvoering van een opdracht of bij de voltooiing ervan.

21. Wanneer de contractant of subcontractant gemachtigd is gerubriceerde informatie te houden na voltooiing van een opdracht, blijven de minimumnormen van dit besluit van toepassing en wordt de vertrouwelijkheid van gerubriceerde informatie door de contractant of subcontractant beschermd.

22. De voorwaarden waaronder een contractant een beroep kan doen op subcontractanten worden in de aanbesteding en de opdracht omschreven.

23. Een contractant krijgt van het Europees Parlement, als aanbestedende instantie, toestemming voordat hij delen van een gerubriceerde opdracht uitbesteedt aan een onderaannemer. Industriële of andere entiteiten die geregistreerd zijn in een derde land dat geen informatiebeveiligingsovereenkomst met de Europese Unie heeft, mogen niet als subcontractant worden ingeschakeld.

24. Het is de verantwoordelijkheid van de contractant te garanderen dat alle onderaannemingsactiviteiten verlopen in overeenstemming met de minimumnormen van dit besluit en de contractant mag geen gerubriceerde EU-informatie doorgeven aan een subcontractant zonder voorafgaande schriftelijke toestemming van de aanbestedende instantie.

25. Wat betreft gerubriceerde informatie die door de contractant of subcontractant wordt gegenereerd of verwerkt, oefent de aanbestedende instantie de rechten van de opsteller uit.

## E. **BEZOEKEN IN VERBAND MET GERUBRICEERDE OPRACHTEN**

26. Wanneer het Europees Parlement, contractanten of subcontractanten voor de uitvoering van een gerubriceerde opdracht in elkaars ruimten toegang vragen tot als „CONFIDENTIEL UE/EU CONFIDENTIAL" of „SECRET UE/EU SECRET" gerubriceerde informatie, worden in overleg met de nationale veiligheidsinstanties of een andere bevoegde veiligheidsinstantie bezoeken georganiseerd. In het kader van specifieke projecten kunnen de nationale veiligheidsinstanties echter ook een procedure overeenkomen waarmee zulke bezoeken rechtstreeks kunnen worden georganiseerd.

27. Alle bezoekers beschikken over een passende personeelsveiligheidsmachtiging en hebben een noodzaak tot kennisname voor toegang tot de gerubriceerde informatie met betrekking tot de opdracht van het Europees Parlement.

28. Bezoekers krijgen uitsluitend toegang tot de gerubriceerde informatie die verband houdt met het doel van het bezoek.

## F. **OVERDRACHT EN VERVOER VAN GERUBRICEERDE INFORMATIE**

29. Op de overdracht van gerubriceerde informatie met elektronische middelen zijn de desbetreffende bepalingen van veiligheidsmededeling 3 van toepassing.

30. Op het vervoer van gerubriceerde informatie zijn de desbetreffende bepalingen van veiligheidsmededeling 4 en de desbetreffende instructies voor behandeling van toepassing.

31. Wat het vervoer van gerubriceerd materiaal als vracht betreft, worden bij het opstellen van beveiligingsregelingen de volgende beginselen toegepast:

a) de beveiliging wordt tijdens alle fasen van het vervoer gewaarborgd, van het punt van oorsprong tot de eindbestemming;

b) de mate van bescherming die aan een zending wordt verleend, wordt bepaald door de hoogste rubriceringsgraad van het materiaal dat zij bevat;

c) er wordt een VMV op het passende niveau verkregen voor de ondernemingen die het vervoer verzorgen. In dat geval moeten de personeelsleden die de zending verwerken, in overeenstemming met bijlage I een veiligheidsonderzoek ondergaan;

d) vóór iedere grensoverschrijdende verplaatsing van materiaal dat als „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" of op een gelijkwaardig niveau is gerubriceerd, stelt de verzender een vervoerplan op, dat wordt goedgekeurd door de secretaris-generaal;

e) de reizen geschieden zoveel mogelijk vanuit een gegeven startpunt tot een gegeven bestemming, en worden zo snel als de omstandigheden toelaten uitgevoerd;

f) waar mogelijk leiden de routen door het grondgebied van lidstaten.

G. **OVERDRACHT VAN GERUBRICEERDE INFORMATIE NAAR CONTRACTANTEN IN DERDE LANDEN**

32. Gerubriceerde informatie wordt overgedragen aan contractanten en subcontractanten in derde landen overeenkomstig de beveiligingsmaatregelen die zijn overeengekomen door het Europees Parlement, als aanbestedende dienst, en de derde staat in kwestie waar de contractant is geregistreerd.

H. **BEHANDELING EN OPSLAG VAN INFORMATIE MET RUBRICERING „RESTREINT UE/EU RESTRICTED"**

33. Samen, waar nodig, met de nationale veiligheidsinstantie van de betrokken lidstaat, is het Europees Parlement, als aanbestedende instantie, op basis van contractuele bepalingen gerechtigd bezoeken af te leggen aan vestigingen van contractanten/subcontractanten om na te gaan of, zoals in de opdracht wordt vereist, de beveiligingsmaatregelen ter zake zijn getroffen voor de bescherming van gerubriceerde EUCI van het niveau „RESTREINT UE/EU RESTRICTED".

34. Voor zover dat nodig is volgens de nationale wet- en regelgeving, worden nationale veiligheidsinstanties of andere bevoegde veiligheidsinstanties door het Europees Parlement, als aanbestedende dienst, in kennis gesteld van opdrachten of opdrachten in onderaanneming die informatie met de rubricering „RESTREINT UE/EU RESTRICTED" bevatten.

35. Een VMV of een PMV voor contractanten of subcontractanten en hun personeel is niet vereist voor opdrachten van het Europees Parlement, die als „RESTREINT UE/EU RESTRICTED" gerubriceerde informatie bevatten.

36. Het Europees Parlement bestudeert, als aanbestedende dienst, de reacties op de uitnodigingen tot inschrijving voor opdrachten waarvoor toegang tot als „RESTREINT UE/EU RESTRICTED" gerubriceerde informatie nodig is, ongeacht eventuele vereisten met betrekking tot VMV's of PMV's uit hoofde van nationale wet- en regelgeving.

37. De voorwaarden waaronder een contractant een beroep kan doen op subcontractanten worden in de aanbesteding en de opdracht omschreven.

38. Wanneer een opdracht de verwerking van informatie met rubricering „RESTREINT UE/EU RESTRICTED" in een door een contractant geëxploiteerd CIS behelst, zorgt het Europees Parlement, als aanbestedende dienst, ervoor dat in het contract of de onderaanneming de nodige technische en administratieve eisen worden gespecificeerd met betrekking tot de homologatie van het CIS in overeenstemming met het ingeschatte risico, rekening houdend met alle belangrijke factoren. Hoe ver de homologatie van een dergelijk CIS reikt, wordt door de aanbestedende dienst en de betrokken nationale veiligheidsinstantie bepaald.

**VEILIGHEIDSMEDEDELING 6**

INBREUK OP DE BEVEILIGING, VERLIES OF COMPROMITTERING VAN GERUBRICEERDE INFORMATIE

1. Een inbreuk op de veiligheidsvoorschriften is het resultaat van een handeling of een nalatigheid, in strijd met dit besluit, die vertrouwelijke informatie in gevaar kan brengen of compromitteren.

2. Compromittering van vertrouwelijke informatie doet zich voor wanneer het zeker of aannemelijk is dat zulke gegevens geheel of gedeeltelijk in het bezit zijn gekomen van onbevoegden, d.w.z. personen die geen machtiging of noodzaak tot kennisname hebben.

3. Vertrouwelijke informatie kan gecompromitteerd zijn als gevolg van slordigheid, onachtzaamheid of indiscretie, alsmede door activiteiten van diensten die gericht zijn tegen de EU of door subversieve organisaties.

4. Indien de secretaris-generaal een bewezen of vermoedelijke veiligheidsinbreuk of het verlies of de compromittering van vertrouwelijke informatie ontdekt of daarvan in kennis wordt gesteld, doet hij het nodige om:

a) de feiten vast te stellen;

b) de aangerichte schade te beoordelen en te beperken;

c) herhaling te voorkomen;

d) de bevoegde autoriteit van het derde land of de lidstaat waarvan de vertrouwelijke informatie afkomstig is of dat de vertrouwelijke informatie heeft doorgestuurd, op de hoogte te stellen.

Wanneer er een lid van het Europees Parlement bij een en ander is betrokken, treedt de secretaris-generaal samen met de Voorzitter van het Europees Parlement op.

Wanneer de informatie is ontvangen van de andere instellingen van de Unie, treedt de secretaris-generaal op in overeenstemming met de toepasselijke beveiligingsmaatregelen voor gerubriceerde informatie en de regelingen die zijn vastgesteld in het kader van het Kaderakkoord met de Commissie of de Interinstitutioneeel Akkoord met de Raad.

5. Alle personen die met vertrouwelijke informatie in aanraking komen, worden grondig geïnformeerd over veiligheidsprocedures, de gevaren van indiscrete gesprekken en hun betrekkingen met de media, en ondertekenen indien toepasselijk een verklaring dat zij de inhoud van de vertrouwelijke informatie niet zullen vrijgeven aan derden, dat zij de verplichting gerubriceerde informatie te beschermen zullen nakomen, en dat zij de gevolgen van eventuele niet-nakoming daarvan zullen aanvaarden. Toegang tot en gebruik van gerubriceerde informatie door een persoon die niet is geïnformeerd en die de bijbehorende verklaring niet heeft ondertekend, wordt als een inbreuk op de veiligheidsvoorschriften beschouwd.

6. Leden en ambtenaren van het Europees Parlement en andere parlementaire medewerkers die in dienst van een fractie zijn of contractanten, stellen de secretaris-generaal onmiddellijk op de hoogte van iedere inbreuk op de beveiligingsvoorschriften, ieder verlies of iedere compromittering van vertrouwelijke informatie waarvan zij kennis krijgen.

7. Eenieder die verantwoordelijk is voor het compromitteren van vertrouwelijke informatie stelt zich bloot aan disciplinaire maatregelen, overeenkomstig de geldende regels en voorschriften. Deze maatregelen sluiten verdere gerechtelijke actie niet uit, in overeenstemming met de geldende wetten.

8. Inbreuken die zijn begaan door ambtenaren van het Europees Parlement en andere parlementaire medewerkers die in dienst van een fracties zijn leiden, zonder verdere gerechtelijke actie uit te sluiten, tot de toepassing van de procedures en sancties die in titel VI van het Statuut zijn vastgelegd.

9. Onverminderd verdere gerechtelijke actie, worden inbreuken die zijn begaan door leden van het Europees Parlement, behandeld in overeenstemming met artikel 9, lid 2, en de artikelen 152, 153 en 154 van het Reglement van het Parlement.