Journal officiel de l'Union européenne

C 126

Édition de langue française

Communications et informations

61e année

10 avril 2018

Sommaire

FR

IV

(Informations)

INFORMATIONS PROVENANT DES INSTITUTIONS, ORGANES ET ORGANISMES DE L'UNION EUROPÉENNE

SERVICE EUROPÉEN POUR L'ACTION EXTÉRIEURE

Décision de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité du 19 septembre 2017 relative aux règles de sécurité applicables au Service européen pour l'action extérieure

ADMIN(2017) 10

(2018/C 126/01)

LA HAUTE REPRÉSENTANTE DE L'UNION POUR LES AFFAIRES ÉTRANGÈRES ET LA POLITIQUE DE SÉCURITÉ,

vu la décision 2010/427/UE du Conseil du 26 juillet 2010 fixant l'organisation et le fonctionnement du Service européen pour l'action extérieure ([1]) (ci-après le «SEAE»),

vu les recommandations du comité visé à l'article 9, paragraphe 6, de la décision de la haute représentante du 15 juin 2011 relative aux règles de sécurité applicables au Service européen pour l'action extérieure ([2]),

considérant ce qui suit:

(1) En tant qu'organe de l'Union européenne fonctionnant de manière autonome, le SEAE devrait être doté de règles de sécurité, telles que visées à l'article 10, paragraphe 1, de la décision 2010/427/UE du Conseil.

(2) La haute représentante de l'Union pour les affaires étrangères et la politique de sécurité (ci-après la «haute représentante» ou «HR») doit fixer pour le SEAE des règles de sécurité englobant tous les aspects de la sécurité pour ce qui est du fonctionnement du SEAE, afin que ce dernier soit en mesure de gérer efficacement les risques menaçant son personnel, ses biens matériels, les informations qu'il détient et ses visiteurs et de s'acquitter des responsabilités qui lui incombent en ce qui concerne l'obligation de vigilance à cet égard.

(3) Il convient, en particulier, de garantir au personnel du SEAE, à ses biens matériels, y compris les systèmes d'information et de communication qu'il possède, aux informations qu'il détient et à ses visiteurs un niveau de protection conforme aux meilleures pratiques en usage au Conseil, à la Commission européenne, dans les États membres et, s'il y a lieu, dans les organisations internationales.

(4) Les règles de sécurité applicables au SEAE devraient contribuer à la mise en place d'un cadre général complet et plus cohérent au sein de l'Union européenne pour ce qui est de la protection des informations classifiées de l'UE (ci-après les «ICUE»), en s'appuyant sur les règles de sécurité du Conseil de l'Union européenne (ci-après le «Conseil») et sur les dispositions de la Commission européenne en matière de sécurité, tout en veillant à maintenir la plus grande cohérence possible avec ces règles et dispositions.

(5) Le SEAE, le Conseil et la Commission sont résolus à appliquer des normes équivalentes de sécurité pour protéger les ICUE.

(6) La présente décision est arrêtée sans préjudice des articles 15 et 16 du traité sur le fonctionnement de l'Union européenne (TFUE), ni des instruments les mettant en œuvre.

([1]) JO L 201 du 3.8.2010, p. 30.
([2]) JO C 304 du 15.10.2011, p. 7.

(7) Il importe de fixer l'organisation de la sécurité dans le SEAE et l'allocation des tâches relatives à la sécurité au sein des structures du SEAE.

(8) La haute représentante doit s'appuyer, en fonction des besoins, sur les compétences techniques existant en la matière dans les États membres, au Secrétariat général du Conseil et à la Commission européenne.

(9) La haute représentante doit prendre toutes les mesures qui s'imposent pour appliquer ces règles avec l'appui des États membres, du Secrétariat général du Conseil et de la Commission européenne.

(10) Le secrétaire général du SEAE est l'autorité de sécurité du SEAE, et l'article premier de la décision ADMIN (2015)34 du 14 septembre 2015 du secrétaire général du Service européen pour l'action extérieure prévoit que les fonctions de sécurité de l'autorité de sécurité, telles que prévues par les règles de sécurité du SEAE, sont exercées par le directeur général pour le budget et l'administration,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Objet et champ d'application

La présente décision arrête les règles de sécurité applicables au Service européen pour l'action extérieure (ci-après les «règles de sécurité applicables au SEAE»).

Conformément à l'article 10, paragraphe 1, de la décision 2010/427/UE du Conseil du 26 juillet 2010 fixant l'organisation et le fonctionnement du Service européen pour l'action extérieure, elle s'applique à l'ensemble du personnel du SEAE et à tous les membres du personnel des délégations de l'Union, indépendamment de leur statut administratif ou origine, et instaure le cadre réglementaire général en vue de gérer efficacement les risques pesant sur le personnel relevant de la responsabilité du SEAE tel que visé à l'article 2, les locaux du SEAE, ses biens matériels, les informations qu'il détient et ses visiteurs.

Article 2

Définitions

Aux fins de la présente décision, on entend par:

a) «membres du personnel du SEAE»: les fonctionnaires et autres agents du SEAE, y compris le personnel des services diplomatiques des États membres nommés comme agents temporaires, les experts nationaux détachés, tels que définis à l'article 6 de la décision 2010/427/UE du Conseil du 26 juillet 2010 fixant l'organisation et le fonctionnement du Service européen pour l'action extérieure;

b) «membres du personnel placés sous la responsabilité du SEAE»: les membres du personnel du SEAE au siège et dans les délégations de l'Union, ainsi que tous les autres membres du personnel des délégations de l'Union, indépendamment de leur statut administratif ou origine, ainsi que, aux fins de la présente décision, la haute représentante et, le cas échéant, d'autres membres du personnel résidant au siège du SEAE;

c) «personnes à charge»: les membres de la famille du personnel placé sous la responsabilité du SEAE dans les délégations de l'Union, qui composent leur propre ménage tel qu'il a été notifié au ministère des affaires étrangères de l'État d'accueil;

d) «locaux du SEAE»: tous les établissements du SEAE, y compris les bâtiments, bureaux, salles et autres espaces, ainsi que les lieux hébergeant des systèmes d'information et de communication (dont les équipements de traitement des ICUE), où le SEAE exerce des activités permanentes ou temporaires;

e) «intérêts du SEAE à protéger»: les membres du personnel placés sous la responsabilité du SEAE, les locaux, les personnes à charge, les biens matériels, y compris les systèmes d'information et de communication, les informations et les visiteurs du SEAE;

f) «informations classifiées de l'UE» (ICUE): toute information ou tout matériel identifié comme tel par une classification de sécurité de l'UE, dont la divulgation non autorisée pourrait porter atteinte à des degrés divers aux intérêts de l'Union européenne, ou à ceux d'un ou de plusieurs de ses États membres;

g) «délégation de l'Union»: les délégations auprès des pays tiers et des organisations internationales visées à l'article 1er, paragraphe 4, de la décision 2010/427/UE du Conseil du 26 juillet 2010 fixant l'organisation et le fonctionnement du Service européen pour l'action extérieure.

D'autres définitions figurent dans les annexes pertinentes et à l'appendice A.

Article 3

Devoir de diligence

1. Les règles de sécurité applicables au SEAE ont pour but de lui permettre d'assumer ses responsabilités au regard du devoir de diligence.

2. Le devoir de diligence incombant au SEAE comprend la saine diligence consistant à prendre toutes les mesures raisonnables pour mettre en œuvre les mesures de sécurité visant à empêcher tout préjudice raisonnablement prévisible aux intérêts du SEAE à protéger.

Il comprend à la fois un volet sécurité et un volet sûreté, y compris les éléments de ce type résultant des situations d'urgence ou crises, de quelque nature que ce soit.

3. Compte tenu du devoir de diligence incombant aux États membres, aux institutions ou organes de l'UE et à d'autres parties dont le personnel travaille dans des délégations de l'Union et/ou dans les locaux de délégations de l'Union, ou du devoir de diligence incombant au SEAE lorsque des délégations de l'Union sont hébergées dans les locaux d'autres parties susmentionnées, le SEAE conclut, avec chacune des entités susmentionnées, des arrangements administratifs traitant des rôles et responsabilités, tâches et mécanismes de coopération respectifs.

Article 4

Sécurité physique et sécurité des infrastructures

1. Le SEAE met en place toutes les mesures de sécurité physique appropriées (permanentes ou temporaires), y compris les dispositions de contrôle d'accès, pour l'ensemble des locaux du SEAE, aux fins de la préservation des intérêts du SEAE à protéger. De telles mesures entrent en ligne de compte lors de la conception et de la planification de nouveaux locaux ou avant la location à bail de locaux existants.

2. Des obligations ou restrictions spéciales peuvent être imposées aux membres du personnel placés sous la responsabilité du SEAE et aux personnes à charge, pour des raisons de sécurité, pendant une période donnée et dans des domaines précis.

3. Les mesures visées aux paragraphes 1 et 2 doivent être proportionnées au risque évalué.

Article 5

États d'alerte et gestion des situations de crise

1. L'autorité de sécurité du SEAE telle que définie à l'article 13, paragraphe 1, section I, est chargée de mettre en place les mesures d'état d'alerte appropriées à titre d'anticipation ou de riposte face à des menaces et des incidents affectant la sécurité au sein du SEAE, ainsi que les mesures requises pour gérer les situations de crise.

2. Les mesures d'état d'alerte visées au paragraphe 1 doivent être proportionnées au niveau de menace pour la sécurité. Les niveaux d'état d'alerte sont définis en étroite coopération avec les services compétents des autres institutions, agences et organes de l'Union et ceux de l'État membre ou des États membres accueillant les locaux du SEAE.

3. L'autorité de sécurité du SEAE fait office de point de contact pour les états d'alerte et la gestion des situations de crise.

Article 6

Protection des informations classifiées

1. La protection des ICUE est régie par les exigences formulées dans la présente décision, et notamment dans l'annexe A. Le détenteur de toute ICUE est tenu de la protéger en conséquence.

2. Le SEAE veille à ce que seules les personnes réunissant les conditions exposées à l'article 5 de l'annexe A aient accès aux informations classifiées.

3. Les conditions auxquelles les agents locaux peuvent avoir accès aux ICUE sont également fixées par la haute représentante, conformément aux règles de protection des ICUE établies à l'annexe A de la présente décision.

4. La direction du SEAE chargée de la sécurité gère une base de données concernant l'habilitation de sécurité de tous les membres du personnel placés sous la responsabilité du SEAE et de ses contractants.

5. Lorsque les États membres introduisent des informations classifiées portant un marquage national de classification de sécurité dans les structures ou réseaux du SEAE, ce dernier protège ces informations conformément aux règles applicables aux ICUE de niveau équivalent tel que prévu dans le tableau d'équivalence des classifications de sécurité figurant à l'appendice B de la présente décision.

6. Les zones du SEAE où sont stockées des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, ou équivalent, sont créées en tant que zones sécurisées conformément aux règles applicables en vertu de l'annexe AII de la présente décision, et doivent être approuvées par l'autorité de sécurité du SEAE.

7. Les procédures d'habilitation à l'exécution de tâches incombant à la haute représentante dans le cadre d'accords ou d'arrangements administratifs concernant l'échange d'ICUE avec des pays tiers ou des organisations internationales sont décrites aux annexes A et A VI de la présente décision.

8. Le secrétaire général détermine les conditions dans lesquelles le SEAE peut échanger les ICUE qu'il détient avec d'autres institutions, organes, organismes ou agences de l'Union européenne. Un cadre approprié sera mis en place à cette fin, y compris au moyen de la conclusion d'accords interinstitutionnels ou d'autres arrangements lorsque cela est nécessaire à cet effet.

9. Un tel cadre vise à garantir que les ICUE font l'objet d'une protection appropriée à leur niveau de classification et conforme à des principes de base et normes minimales équivalents à ceux énoncés dans la présente décision.

Article 7

Incidents et urgences en matière de sécurité

1. Afin de garantir une réponse opportune et efficace aux incidents en matière de sécurité, le SEAE établit une procédure de signalement de tels incidents et urgences, qui soit opérationnelle 24 heures sur 24, sept jours sur sept, et couvre tout type d'incident en matière de sécurité ou de menace pour les intérêts du SEAE à protéger (par exemple accidents, conflits, actes malveillants, actes criminels, enlèvements et prises d'otages, urgences médicales, incidents au niveau des systèmes d'information et de communication, cyberattaques, etc.).

2. Des lignes d'urgence sont établies entre le siège du SEAE, les délégations de l'Union, le Conseil, la Commission, les représentants spéciaux de l'UE et les États membres, afin de les aider à gérer les incidents sur le plan de la sécurité impliquant du personnel et leurs conséquences, y compris la planification des mesures d'urgence.

3. Cette gestion des incidents de sécurité inclut, entre autres:

— des procédures de soutien efficace au processus décisionnel en cas d'incident de sécurité impliquant du personnel, y compris des décisions liées à l'extraction ou à la suspension d'une mission, et

— une politique et des procédures de récupération du personnel, par exemple en cas de disparitions ou en cas d'enlèvements ou de prises d'otages, en tenant compte des responsabilités particulières des États membres, des institutions de l'UE et du SEAE à cet égard. La nécessité de disposer de capacités spécifiques, dans le cadre de la gestion de telles opérations sur ce point, est prise en considération eu égard aux ressources que les États membres pourraient fournir.

4. Le SEAE met en place des arrangements administratifs en matière de signalement de tout incident de sécurité survenant dans les délégations de l'Union. Les États membres, la Commission, tout autre autorité pertinente, ainsi que les comités de sécurité concernés sont informés, le cas échéant.

5. Les procédures de gestion des incidents devraient être mises à l'épreuve et réexaminées régulièrement.

Article 8

Sécurité des systèmes d'information et de communication

1. Le SEAE protège les informations traitées dans les systèmes d'information et de communication (ci-après «SIC») contre les menaces pesant sur leur confidentialité, leur intégrité, leur disponibilité, leur authenticité et leur non-répudiation.

2. L'autorité de sécurité du SEAE approuve des règles, des lignes directrices en matière de sécurité et un programme de sécurité pour la protection de tous les SIC détenus ou exploités par le SEAE.

3. Les règles, la politique et le programme sont conformes à ceux du Conseil et de la Commission et, le cas échéant, aux politiques de sécurité appliquées par les États membres, et leur mise en œuvre est étroitement coordonnée avec ces derniers.

4. Tous les SIC traitant des informations classifiées font l'objet d'un processus d'homologation. Le SEAE applique un système de gestion de l'homologation de sécurité en concertation avec le Secrétariat général du Conseil et la Commission européenne.

5. Lorsque la protection des ICUE traitées par le SEAE est assurée par des produits cryptographiques, ces produits doivent être agréés par l'autorité d'agrément cryptographique du SEAE, sur recommandation du comité de sécurité du Conseil.

6. L'autorité de sécurité du SEAE met en place, selon les besoins, les autorités chargées de l'assurance de l'information, comme suit:

a) une autorité chargée de l'assurance de l'information;

b) une autorité TEMPEST;

c) une autorité d'agrément cryptographique;

d) une autorité de distribution cryptographique.

7. Pour chaque système, l'autorité de sécurité du SEAE crée les autorités suivantes:

a) une autorité d'homologation de sécurité;

b) une autorité opérationnelle chargée de l'assurance de l'information.

8. Les dispositions d'application du présent article concernant la protection des ICUE sont exposées aux annexes A et A IV.

Article 9

Infractions à la sécurité et compromission des informations classifiées

1. Une infraction à la sécurité résulte d'un acte ou d'une omission qui est contraire aux règles de sécurité énoncées dans la présente décision et/ou aux politiques ou lignes directrices en matière de sécurité énonçant les éventuelles mesures nécessaires à sa mise en œuvre, telles qu'approuvées conformément à l'article 21, paragraphe 1.

2. Une compromission d'informations classifiées consiste en une divulgation totale ou partielle desdites informations à des personnes ou entités non autorisées.

3. Toute infraction à la sécurité, réelle ou présumée, et toute compromission d'informations classifiées, réelle ou présumée, sont immédiatement signalées à la direction du SEAE chargée de la sécurité, qui prend les mesures appropriées, telles qu'énoncées à l'annexe A, article 11.

4. Toute personne coupable d'une infraction aux règles de sécurité établies dans la présente décision, ou d'une compromission d'informations classifiées, est passible d'une sanction disciplinaire et/ou juridique, conformément aux dispositions législatives et réglementaires applicables, telles qu'énoncées à l'article 11, paragraphe 3, de l'annexe A.

Article 10

Enquêtes sur les incidents de sécurité, infractions et/ou compromissions et actions correctives

1. Sans préjudice de l'article 86 (régime disciplinaire) et de l'annexe IX du statut ([1]), les enquêtes de sécurité peuvent être menées par la direction du SEAE chargée de la sécurité:

a) en cas de fuite, usage abusif ou compromission potentiels d'informations sensibles non classifiées, d'ICUE ou d'informations classifiées Euratom;

b) pour contrer les attaques hostiles de services de renseignement contre le SEAE et son personnel;

c) pour contrer les attaques terroristes contre le SEAE et son personnel;

d) en cas de cyberincidents;

e) en cas d'autres incidents touchant ou susceptibles de toucher la sécurité générale au sein du SEAE, y compris en cas de suspicion d'infractions pénales.

2. La direction du SEAE chargée de la sécurité, assistée d'experts des États membres et/ou d'autres institutions de l'Union, le cas échéant, et moyennant l'autorisation de l'autorité de sécurité du SEAE, si besoin est, met en œuvre toute action corrective nécessaire résultant d'enquêtes, lorsqu'il y a lieu.

Seul le personnel autorisé sur la base d'un mandat nominatif attribué par l'autorité de sécurité du SEAE, compte tenu de ses obligations actuelles, peut être habilité à mener et coordonner des enquêtes de sécurité dans le cadre du SEAE.

3. Les enquêteurs ont accès à toutes les informations nécessaires à la conduite de telles enquêtes et bénéficient de toute l'aide de l'ensemble des services et du personnel du SEAE sur ce point.

Les enquêteurs peuvent entreprendre des actions adéquates pour préserver les preuves réunies d'une manière proportionnée à la gravité du cas examiné.

4. Lorsque l'accès aux informations a trait à des données à caractère personnel, y compris celles contenues dans les systèmes d'information et de communication, un tel accès respectera les dispositions du règlement (CE) n° 45/2001 ([2]).

5. En cas de nécessité d'établir une base de données d'investigation qui contiendra des données à caractère personnel, le Contrôleur européen de la protection des données (CEPD) en est informé conformément au règlement précité.

Article 11

Gestion des risques de sécurité

1. Afin de déterminer ses besoins en matière de sécurité, le SEAE élabore une méthode globale d'évaluation des risques pour la sécurité, en étroite coopération avec la direction de la sécurité de la Commission et, le cas échéant, avec le bureau de sécurité du Secrétariat général du Conseil.

2. Les risques pesant sur les intérêts du SEAE à protéger sont gérés dans le cadre d'une procédure. Cette dernière vise à déterminer les risques connus pesant sur la sécurité, à définir des mesures de sécurité permettant de ramener ces risques à un niveau acceptable et à appliquer ces mesures selon le principe de défense en profondeur. L'efficacité de telles mesures et le niveau de risque font l'objet d'une évaluation constante.

([1]) Statut des fonctionnaires de l'Union européenne et régime applicable aux autres agents de l'Union européenne, fixés dans le règlement (CEE, Euratom, CECA) n° 259/68 du Conseil (JO L 56 du 4.3.1968, p. 1), ci-après le «statut».

([2]) Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

3. Les rôles, responsabilités et tâches fixés dans la présente décision sont sans préjudice de la responsabilité qui incombe à chaque membre du personnel placé sous la responsabilité du SEAE; plus particulièrement, les membres du personnel de l'UE en mission dans des pays tiers doivent faire preuve de bon sens et de discernement pour ce qui a trait à leur propre sécurité, et respecter toutes les dispositions législatives et réglementaires, procédures et consignes de sécurité applicables.

4. Afin de prévenir et contrôler les risques de sécurité, le personnel mandaté peut effectuer une vérification des antécédents des personnes entrant dans le champ d'application de la présente décision, de manière à déterminer si l'octroi à ces personnes de l'accès aux locaux ou à des informations du SEAE représente une menace pour la sécurité. À cette fin, et conformément au règlement (CE) nº 45/2001, le personnel mandaté concerné peut: a) utiliser toutes les sources d'information dont dispose le SEAE, en tenant compte de la fiabilité de la source d'information; b) accéder au fichier du personnel ou aux données détenues par le SEAE concernant les personnes qu'il emploie ou envisage d'employer, ou pour le personnel des contractants lorsque cela est dûment justifié.

5. Le SEAE prend toutes les mesures raisonnables pour garantir la sécurité de ses intérêts qui doivent être protégés et pour éviter tout dommage raisonnablement prévisible s'y rapportant.

6. Les mesures de sécurité applicables au SEAE visant à protéger les ICUE tout au long de leur cycle de vie sont proportionnées en particulier à leur classification de sécurité, à la forme sous laquelle se présentent les informations ou les matériels ainsi qu'à leur volume, au lieu et à la construction des établissements où se trouvent des ICUE et à la menace, notamment celle évaluée à l'échelle locale, que représentent les activités malveillantes et/ou criminelles, y compris l'espionnage, le sabotage et le terrorisme.

Article 12

Sensibilisation et formation en matière de sécurité

1. L'autorité de sécurité du SEAE veille à l'élaboration et à la mise en œuvre de programmes de sensibilisation et de formation en matière de sécurité au sein du SEAE et fait en sorte que les membres du personnel placés sous la responsabilité du SEAE et, s'il y a lieu, les personnes à leur charge, bénéficient des actions de formation et de sensibilisation nécessaires et proportionnées aux risques inhérents à leur lieu de résidence.

2. Avant de se voir accorder l'accès à des ICUE et à intervalles réguliers par la suite, le personnel est informé des responsabilités qui lui incombent en matière de protection des ICUE, conformément aux règles applicables en vertu de l'article 6, et reconnaît ces responsabilités.

Article 13

Organisation de la sécurité au sein du SEAE

Section 1

Dispositions générales

1. Le secrétaire général est l'autorité de sécurité du SEAE. En cette qualité, le secrétaire général veille:

a) à ce que les mesures de sécurité fassent l'objet, si nécessaire, d'une coordination avec les autorités compétentes des États membres, le Secrétariat général du Conseil, la Commission européenne et, s'il y a lieu, les pays tiers ou organisations internationales sur toutes les questions de sécurité présentant un intérêt pour les activités du SEAE, notamment en ce qui concerne la nature des risques qui pèsent sur les intérêts du SEAE à protéger et les moyens pour ce faire;

b) à ce que les aspects liés à la sécurité soient pleinement pris en compte d'emblée pour l'ensemble des activités du SEAE;

c) à ce que seules les personnes réunissant les conditions exposées à l'article 5 de l'annexe A aient accès aux informations classifiées;

d) à ce que soit établi un système d'enregistrement qui garantisse que les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur soient traitées conformément à la présente décision au sein du SEAE, ainsi qu'au sein des États membres de l'UE, des institutions, organes et organismes de l'Union ou d'autres destinataires autorisés si elles leur ont été communiquées. Un registre distinct est tenu pour toutes les ICUE communiquées par le SEAE à des pays tiers ou des organisations internationales, et pour toutes les informations classifiées communiquées par des pays tiers ou des organisations internationales;

e) à ce que les inspections de sécurité visées à l'article 16 soient réalisées;

f) à ce que des enquêtes soient menées sur toute infraction à la sécurité, réelle ou présumée, ainsi que sur toute compromission ou perte — réelle ou présumée — d'informations classifiées détenues par le SEAE ou provenant de ce dernier, et à ce qu'il soit demandé aux autorités de sécurité compétentes de participer à de telles enquêtes;

g) à ce que des mécanismes et des plans adéquats de gestion des incidents et de leurs conséquences soient mis en place, de manière à réagir rapidement et efficacement en cas d'incidents de sécurité;

h) à ce que des mesures appropriées soient prises en cas de non-respect de la présente décision;

i) à ce que des mesures physiques et organisationnelles appropriées soient mises en place pour protéger les intérêts du SEAE qui doivent l'être.

À cet égard, l'autorité de sécurité du SEAE:

— fixe la catégorie de sécurité des délégations de l'Union, en concertation avec la Commission,

— décide, après consultation de la HR, et le cas échéant, de l'évacuation, ou non, du personnel des délégations de l'Union si la sécurité l'exige,

— décide des mesures à appliquer pour la protection des personnes à charge, compte tenu, le cas échéant, des arrangements convenus avec les institutions de l'Union visés à l'article 3, paragraphe 3,

— approuve la politique de communication cryptographique, en particulier le programme d'installation de produits et du mécanisme cryptographiques.

2. L'autorité de sécurité du SEAE est assistée dans cette tâche par le DGBA, par le directeur du SEAE chargé de la sécurité et, le cas échéant, par le secrétaire général adjoint chargé de la PSDC et de la réponse aux crises.

3. Le secrétaire général en tant qu'autorité de sécurité du SEAE peut déléguer des tâches dans ce domaine, le cas échéant.

4. Chaque chef de département/division est tenu de mettre en œuvre les règles de protection des ICUE au sein de son département ou de sa division.

Tout en conservant les responsabilités mentionnées ci-dessus, chaque chef de département/division désigne des membres du personnel pour assurer les fonctions de coordinateur de la sécurité du département/de la division, dont les ressources seront proportionnées au volume d'ICUE traitées par ce département/cette division.

Les coordinateurs de la sécurité du département assistent et soutiennent, le cas échéant, leur chef de département/division dans l'exécution des tâches liées à la sécurité, telles que:

a) l'élaboration de toute exigence de sécurité supplémentaire adaptée aux besoins spécifiques du département/de la division;

b) l'établissement de comptes rendus périodiques sur la sécurité à l'intention des membres de leur département/division;

c) la prise de mesures visant à faire respecter le principe du «besoin d'en connaître» dans leur département/division;

d) la tenue à jour d'une liste de codes et de clés sûrs;

e) le maintien de procédures et de mesures de sécurité;

f) le signalement de toute infraction aux règles de sécurité et/ou de toute compromission d'ICUE tant au directeur qu'à la direction chargée de la sécurité;

g) le débriefing aux membres du personnel qui cessent de travailler pour le SEAE;

h) la fourniture de rapports réguliers, via leur hiérarchie, sur les questions de sécurité du département/de la division;

i) la mise en rapport avec la direction du SEAE responsable de la sécurité sur des questions de sécurité.

Toute activité ou question susceptible d'avoir une incidence sur la sécurité est notifiée à la direction du SEAE responsable de la sécurité en temps utile.

5. Chaque chef de délégation est responsable de la mise en œuvre de l'ensemble des mesures relatives à la sécurité de la délégation de l'Union.

Section 2

La direction du SEAE chargée de la sécurité

1. Le SEAE dispose d'une direction chargée de la sécurité. Elle doit:

a) gérer, coordonner, superviser et/ou mettre en œuvre toutes les mesures de sécurité dans tous les locaux relevant de la responsabilité du SEAE, au siège, à l'intérieur de l'UE et dans les pays tiers;

b) assurer la cohérence par rapport à la présente décision et aux modalités d'application de toute activité qui pourrait avoir une incidence sur la préservation des intérêts du SEAE à protéger;

c) assurer les fonctions de conseiller principal de la HR, de l'autorité de sécurité du SEAE et du secrétaire général adjoint sur toutes les questions relatives à la sécurité;

d) se faire assister par les services compétents des États membres, conformément à l'article 10, paragraphe 3, de la décision 2010/427/UE du Conseil fixant l'organisation et le fonctionnement du SEAE;

e) soutenir les activités de l'autorité d'homologation de sécurité du SEAE en effectuant des évaluations de la sécurité physique de l'environnement général de sécurité (EGS)/de l'environnement local de sécurité (ELS) des systèmes d'information et de communication traitant des ICUE, ainsi que des locaux autorisés à traiter et à stocker des ICUE.

2. Le directeur du SEAE responsable de la sécurité est chargé:

a) de garantir la protection générale des intérêts du SEAE à protéger;

b) de rédiger, de revoir et de mettre à jour les règles de sécurité, ainsi que de coordonner les mesures de sécurité avec les autorités nationales compétentes et, le cas échéant, les autorités compétentes de pays tiers et d'organisations internationales liées à l'UE par des accords et/ou des arrangements de sécurité;

c) d'appuyer les procédures du comité de sécurité du SEAE, tel qu'établi à l'article 15, paragraphe 1, de la présente décision;

d) de se mettre en rapport avec tous partenaires ou autorités autres que ceux mentionnés au point b) ci-dessus pour les questions de sécurité, le cas échéant;

e) d'établir des priorités et de soumettre des propositions en vue de la gestion du budget consacré à la sécurité au siège et dans les délégations de l'Union.

3. Le chef de la direction du SEAE responsable de la sécurité est chargé:

a) de garantir l'enregistrement des infractions et compromissions en matière de sécurité, le lancement et la conduite d'enquêtes dans de tels cas, lorsque c'est nécessaire;

b) de se réunir régulièrement, à chaque fois que c'est nécessaire, avec le directeur de la sécurité du Secrétariat général du Conseil et avec le directeur de la direction de la sécurité de la Commission pour discuter de thèmes d'intérêt commun.

4. La direction du SEAE chargée de la sécurité noue des contacts et entretient une coopération étroite avec:

— les départements responsables de la sécurité au sein des ministères nationaux des affaires étrangères,

— les autorités nationales de sécurité (ANS) et/ou les autres autorités compétentes en matière de sécurité dans les États membres afin d'obtenir leur aide quant aux informations dont elle a besoin pour évaluer les dangers et menaces qui peuvent peser sur le SEAE, son personnel, ses activités, ses biens et ses ressources, ainsi que ses informations classifiées dans les lieux où se déroulent normalement ses travaux,

— les autorités de sécurité compétentes des États membres ou des pays d'accueil sur le territoire desquels le SEAE peut exercer ses activités, concernant toute question relative à la protection des membres de son personnel, de ses activités, de ses biens et ressources, ainsi que de ses informations classifiées quand ils se trouvent sur leur territoire,

— le bureau de sécurité du Secrétariat général du Conseil et la direction de la sécurité de la direction générale des ressources humaines et de la sécurité de la Commission et, le cas échéant, les services chargés de la sécurité des autres institutions, organes et organismes de l'UE,

— les services de sécurité de pays tiers ou d'organisations internationales, aux fins de toute coordination utile, et

— les ANS des États membres, concernant toute question relative à la protection des ICUE.

Section 3

Délégations de l'Union

1. Chaque chef de délégation est responsable de la mise en œuvre et de la gestion, au niveau local, de toutes les mesures relatives à la préservation des intérêts du SEAE à protéger dans les locaux de la délégation de l'Union concernée et relevant de sa compétence.

Il prend, en concertation avec les autorités compétentes de l'État d'accueil si nécessaire, toutes les mesures pouvant être raisonnablement mises en œuvre afin de garantir la mise en place, à cette fin, de mesures physiques et organisationnelles adéquates.

Le chef de délégation établit les procédures de sécurité concernant la protection des personnes à charge, telles que définies à l'article 2, point c), compte tenu, le cas échéant, de tout arrangement administratif visé à l'article 3, paragraphe 3. Le chef de délégation rend compte de toutes les questions de sécurité relevant de sa compétence au chef de la direction du SEAE chargée de la sécurité.

Il est assisté, dans l'accomplissement de ces tâches, par la direction du SEAE chargée de la sécurité, par l'équipe de gestion de la sécurité de la délégation de l'Union, qui est composée d'agents exerçant des tâches et fonctions de sécurité, et par du personnel de sécurité affecté en cas de besoin.

La délégation de l'Union noue des contacts réguliers et entretient une coopération étroite en matière de sécurité avec les missions diplomatiques des États membres.

2. Le chef de délégation prend en outre les mesures suivantes:

— il établit des plans de sécurité et d'urgence détaillés pour la délégation de l'Union, sur la base de procédures opérationnelles standard générales,

— il s'occupe d'un système opérationnel 24 heures sur 24 et 7 jours sur 7 de gestion des incidents de sécurité et des urgences relevant du champ d'intervention de la délégation de l'Union,

— il veille à ce que tous les membres du personnel travaillant pour la délégation de l'Union soient assurés conformément aux conditions en la matière,

— il veille à ce que le thème de la sécurité soit intégré à la formation d'entrée en service que les délégations de l'Union dispensent à tous les membres du personnel au moment de les accueillir, et

— il s'assure de la bonne mise en œuvre des recommandations émises après les évaluations de la sécurité et transmet des rapports écrits à intervalles réguliers au sujet de leur mise en œuvre et d'autres questions de sécurité à l'autorité de sécurité du SEAE.

3. Tout en demeurant responsable et en devant continuer de rendre compte de la préservation de la gestion de la sécurité ainsi que de l'obligation qui lui incombe de garantir la résilience organisationnelle, le chef de délégation peut déléguer l'exécution de ses tâches en matière de sécurité au coordinateur de la sécurité de la délégation (CSD), à savoir soit le chef adjoint de la délégation ou, si personne n'est désigné, quiconque à même d'assurer cette fonction.

Plus particulièrement, les responsabilités suivantes peuvent être confiées au CSD:

— coordonner les fonctions de sécurité au sein de la délégation de l'Union,

— se mettre en rapport, pour les questions de sécurité, avec les autorités compétentes du pays d'accueil et les homologues indiqués au sein des ambassades et des missions diplomatiques des États membres,

— mettre en œuvre des procédures adéquates de gestion de la sécurité en rapport avec les intérêts du SEAE à protéger, y compris la protection des ICUE,

— assurer le respect des règles et instructions de sécurité,

— mettre les membres du personnel au courant des règles de sécurité auxquelles ils doivent se soumettre, ainsi que des risques particuliers dans le pays d'accueil,

— soumettre des demandes à la direction du SEAE chargée des habilitations de sécurité concernant les positions nécessitant une habilitation de sécurité du personnel (HSP), et

— tenir le chef de délégation, le responsable régional de la sécurité (RSO) et la direction du SEAE chargée de la sécurité constamment informés des incidents ou nouveaux éléments en la matière ayant une incidence sur la préservation des intérêts du SEAE à protéger.

4. Le chef de délégation peut déléguer des tâches de sécurité à caractère administratif ou technique au chef d'administration et à d'autres membres du personnel de la délégation de l'Union.

5. La délégation de l'Union est assistée par un RSO. Dans les délégations de l'Union, les RSO endossent les rôles, définis ci-dessous, dans chacun de leurs domaines de compétences géographiques respectifs.

Dans certaines circonstances, lorsque les conditions de sécurité du moment l'exigent, un RSO précis peut être assigné à résider à temps plein dans une délégation de l'Union donnée.

Un RSO peut être muté dans une zone ne relevant pas de son domaine de compétence actuel, y compris au siège, voire devoir accepter un poste résidentiel en fonction de la situation d'un pays en matière de sécurité, et en fonction des exigences de la direction du SEAE chargée de la sécurité.

6. Les RSO sont placés sous le contrôle opérationnel direct du service du siège du SEAE chargé de la sécurité sur le terrain, mais sous le contrôle administratif partagé du chef de délégation de leur lieu d'affectation et du service du siège chargé de la sécurité sur le terrain. Ils conseillent et assistent le chef de délégation et les membres du personnel de la délégation de l'Union dans l'organisation et la mise en œuvre de toutes les mesures physiques, organisationnelles et procédurales liées à la sécurité de la délégation.

7. Les RSO prodiguent conseil et soutien au chef de délégation et au personnel de délégation de l'Union. Lorsqu'il y a lieu, en particulier lorsqu'un RSO est un résident à temps plein dans la délégation, il ou elle devrait aider la délégation de l'Union dans la gestion et la mise en œuvre de la sécurité, y compris dans la préparation de contrats de sécurité, la gestion d'homologations et d'habilitations.

Article 14

Opérations PSDC et représentants spéciaux de l'UE

La direction du SEAE chargée de la sécurité conseille le directeur de la direction «Gestion des crises et planification» (CMPD), le directeur général de l'État-major de l'UE (EMUE), le commandant d'opérations civiles de la Capacité civile de planification et de conduite (CPCC), ainsi que les commandants d'opérations militaires pour ce qui est du volet «sécurité» des opérations de PSDC, et les représentants spéciaux de l'UE en ce qui concerne le volet «sécurité» de leur mandat, complémentaires aux dispositions spécifiques prévues en la matière dans les politiques pertinentes adoptées par le Conseil.

Article 15

Le comité de sécurité du SEAE

1. Un comité de sécurité est créé par la présente décision.

Il est présidé par l'autorité de sécurité du SEAE ou par son délégué désigné et se réunit sur instruction du président ou à la demande de l'un de ses membres. La direction du SEAE chargée de la sécurité assiste le président dans ses fonctions et soutient administrativement, si nécessaire, les délibérations du comité.

2. Le comité de sécurité du SEAE est composé de représentants:

— de chaque État membre,

— du bureau de sécurité du Secrétariat général du Conseil,

— de la direction de la sécurité de la direction générale des ressources humaines et de la sécurité de la Commission européenne.

Une délégation nationale près le comité de sécurité du SEAE peut être composée de membres:

— de l'autorité nationale de sécurité et/ou de l'autorité de sécurité désignée,

— des départements responsables de la sécurité au sein des ministères nationaux des affaires étrangères.

3. Les représentants du comité peuvent être accompagnés et conseillés par des experts selon ce qu'ils jugent nécessaire. Des représentants d'autres institutions, organes ou organismes de l'UE peuvent être invités à y prendre part lorsque des points pertinents pour leur sécurité sont abordés.

4. Sans préjudice du paragraphe 5 ci-dessous, le comité de sécurité du SEAE assiste le SEAE, par voie de consultation, pour toutes les questions de sécurité pertinentes pour les activités du SEAE, le siège et les délégations de l'Union.

Plus particulièrement, et sans préjudice du paragraphe 5 ci-dessous, le comité de sécurité du SEAE:

a) doit être consulté au sujet:

— des politiques, lignes directrices et concepts de sécurité, ainsi que tout autre document de méthodologie concernant la sécurité, notamment en ce qui concerne la protection d'informations classifiées et les mesures à prendre lorsque les membres du personnel du SEAE ne se conforment pas aux règles de sécurité,

— des aspects techniques de sécurité susceptibles d'influencer la décision de la HR de soumettre une recommandation au Conseil en vue de l'ouverture de négociations concernant les accords sur la sécurité des informations visés à l'article 10, paragraphe 1, point a), de l'annexe A,

— de toute modification de la présente décision;

b) peut être consulté ou informé, le cas échéant, au sujet de questions liées à la sécurité de membres du personnel ou de biens au siège du SEAE et dans les délégations de l'Union, sans préjudice de l'article 3, paragraphe 3;

c) doit être informé de toute compromission ou perte d'ICUE se produisant au sein du SEAE.

5. Toute modification des règles relatives à la protection des ICUE contenues dans la présente décision et son annexe A requiert l'avis unanimement favorable des États membres représentés au sein du comité de sécurité du SEAE. Un tel avis unanimement favorable est également requis avant:

— l'ouverture de négociations portant sur les arrangements administratifs visés à l'article 10, paragraphe 1, point b), de l'annexe A,

— la communication d'informations classifiées dans les circonstances exceptionnelles visées aux paragraphes 9, 11 et 12 de l'annexe A VI,

— d'endosser la responsabilité en tant qu'autorité d'origine des informations dans les circonstances visées à l'article 10, paragraphe 6, dernière phrase, de l'annexe A.

Un avis unanimement favorable est obtenu lorsque les délégations des États membres ne formulent aucune objection pendant les délibérations du comité.

6. Le comité de sécurité du SEAE tient pleinement compte des politiques et lignes directrices de sécurité en vigueur au sein du Conseil et de la Commission.

7. Le comité de sécurité du SEAE reçoit la liste des inspections annuelles du SEAE et les rapports d'inspection, dès qu'ils sont finalisés.

8. Organisation des réunions:

— Le comité de sécurité du SEAE se réunit au moins deux fois par an. Des réunions supplémentaires, à part entière ou au format de sécurité ANS/ASD ou MFA, peuvent être convoquées par le président ou organisées à la demande des membres du comité.

— Le comité de sécurité du SEAE organise ses activités de manière à être en mesure de formuler des recommandations sur des aspects spécifiques de la sécurité. Il peut créer d'autres sous-divisions spécialisées, si nécessaire. Il établit le mandat de ces sous-divisions spécialisées et reçoit leurs rapports d'activités.

— La direction du SEAE chargée de la sécurité est tenue de préparer les points de discussion. Le président établit l'ordre du jour provisoire de chaque réunion. Les membres du comité peuvent proposer d'autres points à examiner.

Article 16

Inspections de sécurité

1. L'autorité de sécurité du SEAE veille à ce que les inspections de sécurité soient réalisées, sur une base régulière, au sein du siège du SEAE et des délégations de l'Union afin de vérifier si les mesures de sécurité sont adéquates et si elles sont conformes à la présente décision. La direction du SEAE chargée de la sécurité peut, le cas échéant, désigner des experts qui apporteront leur contribution en participant aux inspections de sécurité dans les organes et organismes de l'Union visés au titre V, chapitre 2, du traité sur l'Union européenne.

2. Les inspections de sécurité du SEAE sont menées sous l'autorité de la direction du SEAE chargée de la sécurité et, le cas échéant, avec le soutien d'experts en sécurité représentant d'autres institutions de l'Union ou États membres, en particulier dans le cadre des arrangements visés à l'article 3, paragraphe 3.

3. Le SEAE peut s'appuyer, si nécessaire, sur les compétences techniques existant en la matière dans les États membres, au Secrétariat général du Conseil et à la Commission européenne.

En cas de besoin, les experts en sécurité compétents basés dans les missions d'États membres dans des pays tiers et/ou des représentants des services de sécurité diplomatiques des États membres peuvent être invités à participer à l'inspection de sécurité au sein de la délégation de l'Union.

4. Les dispositions d'application du présent article concernant la protection des ICUE sont exposées à l'annexe A III.

Article 17

Visites d'évaluation

Des visites d'évaluation sont organisées afin de s'assurer de l'efficacité des mesures de sécurité en place dans un pays tiers ou une organisation internationale pour ce qui est de la protection des ICUE échangées en vertu d'un arrangement administratif tel que visé à l'article 10, paragraphe 1, point b), de l'annexe A.

La direction du SEAE chargée de la sécurité peut demander à des experts d'apporter leur contribution en participant aux visites d'évaluation organisées dans des pays tiers ou des organisations internationales avec lesquels l'UE a conclu un accord sur la sécurité des informations tel que visé à l'article 10, paragraphe 1, point a), de l'annexe A.

Article 18

Planification de la continuité des activités

La direction du SEAE chargée de la sécurité assiste l'autorité de sécurité du SEAE dans la gestion des aspects des processus opérationnels du SEAE se rapportant à la sécurité, dans le cadre de la planification globale de la continuité des activités du SEAE.

Article 19

Consignes en matière de voyages à l'intention des participants à des missions en dehors de l'UE

La direction du SEAE chargée de la sécurité veille à la disponibilité de consignes en matière de voyages à l'intention des membres du personnel placés sous la responsabilité du SEAE amenés à participer à des missions en dehors de l'UE, en exploitant les ressources de tous les services pertinents du SEAE, notamment la salle de veille de l'UE, le centre de situation conjoint de l'Union européenne, les départements géographiques et les délégations de l'Union.

La direction du SEAE chargée de la sécurité fournit sur demande, en puisant dans les ressources susmentionnées, des consignes spécifiques en matière de voyages concernant les missions de membres du personnel placés sous la responsabilité du SEAE dans des pays tiers présentant un niveau de risque élevé ou accru.

Article 20

Santé et sécurité

Les règles de sécurité du SEAE complètent les règles du SEAE en matière de protection de la santé et de la sécurité, telles qu'adoptées par la haute représentante.

Article 21

Mise en œuvre et réexamen

1. L'autorité de sécurité du SEAE approuve, après avoir consulté, le cas échéant, le comité de sécurité du SEAE, les lignes directrices de sécurité fixant les mesures nécessaires à la mise en œuvre de ces règles au sein du SEAE et met en place les capacités nécessaires couvrant tous les aspects de la sécurité, en coopération étroite avec les autorités de sécurité compétentes des États membres et avec le concours des services concernés des institutions de l'Union.

2. Conformément à l'article 4, paragraphe 5, de la décision 2010/427/UE du Conseil du 26 juillet 2010 fixant l'organisation et le fonctionnement du Service européen pour l'action extérieure, des arrangements transitoires peuvent être conclus, si besoin est, au moyen d'accords de niveau de service avec les services compétents du Secrétariat général du Conseil et de la Commission.

3. La HR veille à ce que la présente décision soit appliquée avec cohérence et réexamine périodiquement ces règles de sécurité.

4. Les règles de sécurité du SEAE doivent être mises en œuvre en étroite coopération avec les autorités de sécurité compétentes des États membres.

5. Le SEAE veille à ce que tous les aspects du processus de sécurité soient pris en considération dans le système du SEAE de réaction en cas de crise.

6. Le secrétaire général, en tant qu'autorité de sécurité, et le chef de la direction du SEAE chargée de la sécurité garantissent la mise en œuvre de la présente décision.

Article 22

Remplacement des décisions précédentes

La présente décision abroge et remplace la décision de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité du 19 avril 2013 relative aux règles de sécurité applicables au Service européen pour l'action extérieure ([1]).

Article 23

Dispositions finales

La présente décision entre en vigueur le jour de sa signature.

Elle est publiée au *Journal officiel de l'Union européenne*.

Les autorités compétentes du SEAE informent dûment et en temps utile tous les membres du personnel concernés par la présente décision et ses annexes au sujet de son contenu, de son entrée en vigueur et toute modification qui lui est apportée ultérieurement.

Fait à Bruxelles, le 19 septembre 2017.

Federica MOGHERINI

Haute représentante de l'Union pour les affaires étrangères et la politique de sécurité

([1]) JO C 190 du 29.6.2013, p. 1.

ANNEXE A

PRINCIPES ET NORMES DE PROTECTION DES ICUE

Article premier

Objectif, champ d'application et définitions

1. La présente annexe définit les principes de base et les normes minimales de sécurité pour la protection des ICUE.

2. Ces principes de base et normes minimales s'appliquent au SEAE et aux membres du personnel placés sous sa responsabilité, tels que visés et définis, respectivement, aux articles 1er et 2 de la présente décision.

Article 2

Définition des ICUE, classifications et marquages de sécurité

1. Par «informations classifiées de l'UE» (ICUE), on entend toute information ou tout matériel identifié comme tel par une classification de sécurité de l'UE, dont la divulgation non autorisée pourrait porter atteinte à des degrés divers aux intérêts de l'Union européenne, ou à ceux d'un ou de plusieurs de ses États membres.

2. Les ICUE relèvent de l'un des niveaux de classification suivants:

a) TRÈS SECRET UE/EU TOP SECRET: informations et matériels dont la divulgation non autorisée pourrait causer un préjudice exceptionnellement grave aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres;

b) SECRET UE/EU SECRET: informations et matériels dont la divulgation non autorisée pourrait nuire gravement aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres;

c) CONFIDENTIEL UE/EU CONFIDENTIAL: informations et matériels dont la divulgation non autorisée pourrait nuire aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres;

d) RESTREINT UE/EU RESTRICTED: informations et matériels dont la divulgation non autorisée pourrait être défavorable aux intérêts de l'Union européenne ou d'un ou de plusieurs de ses États membres.

3. Les ICUE portent un marquage de classification de sécurité conformément au paragraphe 2. Elles peuvent porter des marquages supplémentaires pour désigner le domaine d'activité auquel elles sont liées, identifier l'autorité d'origine, limiter la diffusion, restreindre l'utilisation ou indiquer la communicabilité.

Article 3

Gestion de la classification

1. Le SEAE veille à ce que les ICUE soient classifiées de manière appropriée, clairement identifiées en tant qu'informations classifiées, et qu'elles ne conservent leur niveau de classification qu'aussi longtemps que nécessaire.

2. Les ICUE ne sont pas déclassées ni déclassifiées, et aucun des marquages visés à l'article 2, paragraphe 3, n'est modifié ni supprimé sans le consentement écrit préalable de l'autorité d'origine.

3. L'autorité de sécurité du SEAE approuve, après avoir consulté le comité de sécurité du SEAE conformément à l'article 15, paragraphe 5, de la présente décision, les lignes directrices de sécurité relative à la création d'ICUE comprenant un guide de classification pratique.

Article 4

Protection des informations classifiées

1. Les ICUE sont protégées conformément à la présente décision.

2. Il incombe au détenteur de tout élément d'ICUE de le protéger conformément à la présente décision.

3. Lorsque les États membres introduisent des informations classifiées portant un marquage national de classification de sécurité dans les structures ou réseaux du SEAE, ce dernier protège ces informations conformément aux règles applicables aux ICUE de niveau équivalent tel que prévu dans le tableau d'équivalence des classifications de sécurité figurant à l'appendice B.

Le SEAE établit des procédures adéquates afin de tenir des registres précis de l'autorité d'origine

— des informations classifiées que le SEAE reçoit, et

— des sources incluses dans les informations classifiées émanant du SEAE.

Le comité de sécurité du SEAE est informé de ces procédures.

4. Les grandes quantités ou la compilation d'ICUE peuvent justifier un niveau de protection correspondant à une classification plus élevée que celle des éléments qui les composent.

Article 5

Sécurité du personnel amené à traiter des informations classifiées de l'UE

1. La sécurité du personnel passe par l'application de mesures visant à faire en sorte que l'accès aux ICUE ne soit accordé qu'aux personnes qui:

— ont un besoin d'en connaître,

— en ce qui concerne l'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, ont fait l'objet d'une habilitation de sécurité du niveau correspondant, ou ont été dûment autorisées en vertu de leurs fonctions conformément aux dispositions législatives et réglementaires nationales, et

— ont été informées de leurs responsabilités.

2. Les procédures d'habilitation de sécurité concernant le personnel (HSP) ont pour but de déterminer si une personne, compte tenu de sa loyauté, de son intégrité et de sa fiabilité, peut être autorisée à avoir accès à des ICUE.

3. Avant de se voir accorder l'accès à des ICUE et à intervalles réguliers par la suite, toutes les personnes concernées sont informées par écrit des responsabilités qui leur incombent en matière de protection des ICUE conformément à la présente décision et reconnaissent ces responsabilités par écrit.

4. Les modalités d'application du présent article figurent à l'annexe A I.

Article 6

Sécurité physique des informations classifiées de l'UE

1. Par «sécurité physique», on entend l'application de mesures physiques et techniques de protection pour dissuader l'accès non autorisé aux ICUE.

2. Les mesures de sécurité physiques sont destinées à faire obstacle à toute intrusion par la ruse ou par la force, à avoir un effet dissuasif, à empêcher et détecter les actes non autorisés et permettre d'établir une distinction entre les membres du personnel au regard de l'accès aux ICUE conformément au principe du besoin d'en connaître. Ces mesures sont déterminées sur la base d'une procédure de gestion des risques.

3. Les mesures de sécurité physiques sont mises en place pour tous les locaux, bâtiments, bureaux, salles et autres zones dans lesquels des ICUE sont traitées ou stockées, y compris les zones où se trouvent les systèmes d'information et de communication définis à l'article 8, paragraphe 2, de l'annexe A.

4. Des zones où sont stockées des ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont créées en tant que zones sécurisées conformément à l'annexe A II et agréées par l'autorité de sécurité du SEAE.

5. Seuls des équipements ou des dispositifs agréés sont utilisés pour protéger les ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur.

6. Les modalités d'application du présent article figurent à l'annexe A II.

Article 7

Gestion des informations classifiées

1. Par «gestion des informations classifiées», on entend l'application de mesures administratives pour contrôler les ICUE tout au long de leur cycle de vie afin de compléter les mesures prévues aux articles 5, 6 et 8 et de contribuer ainsi à la dissuasion, à la détection et au retour aux conditions opérationnelles dans le cadre de la compromission ou de la perte délibérée ou accidentelle de telles informations. Ces mesures concernent en particulier la création, l'enregistrement, la duplication, la traduction, le transport, le traitement, le stockage et la destruction des ICUE.

2. Les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont enregistrées à des fins de sécurité avant leur diffusion et lors de leur réception. Les autorités compétentes au sein du SEAE établissent un bureau d'ordre à cette fin. Les informations classifiées TRÈS SECRET UE/EU TOP SECRET sont enregistrées dans des bureaux d'ordre désignés.

3. Les services et les locaux dans lesquels les ICUE sont traitées ou stockées font l'objet d'une inspection régulière par l'autorité de sécurité du SEAE.

4. En dehors des zones physiquement protégées, les ICUE sont transmises entre les services et les locaux selon les modalités suivantes:

a) en règle générale, les ICUE sont transmises par voie électronique protégée par des produits cryptographiques agréés conformément à l'article 7, paragraphe 5, de la présente décision et à des procédures d'exploitation de sécurité (SecOP) clairement définies;

b) si la voie visée au point a) n'est pas utilisée, les ICUE sont transportées:

   i) soit sur des supports électroniques (par exemple clé USB, CD, disque dur) protégés par des produits cryptographiques agréés conformément à l'article 8, paragraphe 5, de la présente décision;

   ii) soit, dans tous les autres cas, de la manière prescrite par l'autorité de sécurité du SEAE conformément aux mesures de protection pertinentes prévues à l'annexe A III, section V.

5. Les modalités d'application du présent article figurent à l'annexe A II.

Article 8

Protection d'ICUE traitées dans des systèmes d'information et de communication

1. Par «assurance de l'information (AI) dans le domaine des systèmes d'information et de communication», on entend la certitude que ces systèmes protégeront les informations qu'ils traitent et fonctionneront comme ils le doivent, quand ils le doivent, sous le contrôle d'utilisateurs légitimes. Une AI efficace garantit des niveaux appropriés de confidentialité, d'intégrité, de disponibilité, de non-répudiation et d'authenticité. L'AI est fondée sur un processus de gestion des risques.

2. On entend par «système d'information et de communication» (SIC) tout système permettant le traitement d'informations sous forme électronique. Un système d'information et de communication comprend l'ensemble des moyens nécessaires pour le faire fonctionner, y compris l'infrastructure, l'organisation, le personnel et les ressources d'information. La présente annexe s'applique à tout SIC du SEAE traitant des ICUE.

3. Les SIC traitent des ICUE dans le respect de la notion d'AI.

4. Tous les SIC traitant des ICUE font l'objet d'un processus d'homologation. L'homologation vise à obtenir l'assurance que toutes les mesures de sécurité appropriées ont été mises en œuvre et que les ICUE et les SIC font l'objet d'un niveau suffisant de protection conformément à la présente décision. La déclaration d'homologation détermine le niveau maximal de classification des informations qui peuvent être traitées dans un SIC ainsi que les modalités et les conditions correspondantes.

5. Les SIC traitant des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et d'un niveau de classification supérieur sont protégés de telle manière que les informations ne peuvent pas être compromises par des émissions électromagnétiques non intentionnelles («mesures de sécurité TEMPEST»).

6. Lorsque la protection des ICUE est assurée par des produits cryptographiques, ces produits sont agréés conformément à l'article 8, paragraphe 5, de la présente décision.

7. Lors de la transmission des ICUE par voie électronique, des produits cryptographiques qui ont fait l'objet d'un agrément sont utilisés. Nonobstant cette exigence, des procédures spécifiques peuvent être appliquées en cas d'urgence ou dans le cadre de configurations techniques spécifiques comme le prévoit l'annexe A IV.

8. En vertu de l'article 8, paragraphe 6, de la présente décision, les autorités d'AI suivantes sont établies selon les besoins:

a) une autorité chargée de l'AI (AAI);

b) une autorité TEMPEST (AT);

c) une autorité d'agrément cryptographique (AAC);

d) une autorité chargée de la distribution cryptographique (ADC).

9. En vertu de l'article 8, paragraphe 7, de la présente décision, sont créées, pour chaque système:

a) une autorité d'homologation de sécurité (AHS);

b) une autorité opérationnelle chargée de l'AI.

10. Les modalités d'application du présent article figurent à l'annexe A IV.

Article 9

Sécurité industrielle

1. Par «sécurité industrielle», on entend l'application de mesures visant à assurer la protection des ICUE par des contractants ou des sous-traitants dans le cadre de négociations précontractuelles et tout au long du cycle de vie des contrats classifiés. De manière générale, de tels contrats ne doivent pas concerner l'accès à des informations classifiées TRÈS SECRET UE/EU TOP SECRET.

2. Le SEAE peut, par voie contractuelle, confier à des entités industrielles ou autres immatriculées dans un État membre ou dans un pays tiers ayant conclu un accord sur la sécurité des informations ou un arrangement administratif en vertu de l'article 10, paragraphe 1, de l'annexe A, des tâches qui impliquent ou nécessitent l'accès, le traitement ou le stockage d'ICUE.

3. En tant qu'autorité contractante, le SEAE veille à ce que les normes minimales de sécurité industrielle prévues dans la présente décision et mentionnées dans le contrat soient respectées lors de l'octroi de contrats classifiés à des entités industrielles ou autres. Il garantit le respect de telles normes minimales via l'ANS/ASD concernée.

4. Les contractants et les sous-traitants immatriculés sur le territoire d'un État membre, qui participent à des contrats classifiés ou à des contrats de sous-traitance nécessitant le traitement et le stockage d'informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET au sein de leurs établissements, sont en possession, lors de l'exécution desdits contrats ou durant la phase précontractuelle, d'une habilitation nationale de sécurité d'établissement (HSE) du niveau de classification correspondant délivrée par l'ANS, l'ASD ou toute autre autorité de sécurité compétente dudit État membre.

5. Lorsque les membres du personnel d'un contractant ou d'un sous-traitant doivent, en raison de leurs fonctions aux fins de l'exécution d'un contrat classifié, accéder à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, l'autorité nationale de sécurité (ANS), l'autorité de sécurité désignée (ASD) ou toute autre autorité de sécurité compétente leur délivre une HSP, conformément aux dispositions législatives ou réglementaires nationales et dans le respect des normes minimales définies à l'annexe A I.

6. Les modalités d'application du présent article figurent à l'annexe A V.

Article 10

Échanges d'informations classifiées avec des pays tiers et des organisations internationales

1. Le SEAE ne peut échanger des ICUE avec un pays tiers ou une organisation internationale que dans les cas suivants:

a) un accord sur la sécurité des informations conclu entre l'UE et ce pays tiers ou cette organisation internationale conformément à l'article 37 du TUE et à l'article 218 du TFUE est en vigueur; ou

b) un arrangement administratif, conclu conformément à la procédure énoncée à l'article 15, paragraphe 5, de la présente décision, entre la HR et les autorités de sécurité compétentes de ce pays tiers ou de cette organisation internationale aux fins de l'échange d'informations dont le niveau de classification n'est en principe pas supérieur à RESTREINT UE/EU RESTRICTED, a pris effet; ou

c) un accord-cadre de participation ou un accord de participation ad hoc, conclu en vertu de l'article 37 du traité sur l'Union européenne et de l'article 218 du traité sur le fonctionnement de l'Union européenne, entre l'UE et ce pays tiers dans le cadre d'une opération PESD de gestion de crise est applicable,

et les conditions exposées dans cet instrument sont réunies.

Les exceptions à la règle générale ci-dessus sont précisées à l'annexe A VI, section V.

2. Les arrangements administratifs visés au paragraphe 1, point b), contiennent des dispositions pour garantir que, lorsque des pays tiers ou des organisations internationales reçoivent des ICUE, ces informations bénéficient d'une protection conforme à leur niveau de classification et à des normes minimales qui ne sont pas moins strictes que celles prévues dans la présente décision.

Les informations échangées sur la base des accords visés au paragraphe 1, point c), sont limitées aux informations relatives aux opérations PSDC auxquelles le pays tiers en question participe sur la base de ces accords et conformément à leurs dispositions.

3. Si un accord sur la sécurité des informations est conclu ultérieurement entre l'Union et un État tiers ou une organisation internationale contributeur, l'accord sur la sécurité des informations se substitue aux dispositions relatives à l'échange d'informations classifiées énoncées dans tout accord-cadre de participation, accord de participation ad hoc ou arrangement administratif ad hoc pour ce qui concerne l'échange et le traitement des ICUE.

4. Les ICUE créées aux fins d'une opération PSDC peuvent être divulguées au personnel détaché par des États tiers ou des organisations internationales dans le cadre de cette opération, conformément aux paragraphes 1 à 3, ainsi qu'à l'annexe A VI. Lorsque l'accès aux ICUE est autorisé dans les locaux ou via le SIC d'une opération PSDC, il convient d'appliquer des mesures (y compris l'enregistrement des ICUE divulguées) permettant d'atténuer le risque de perte ou de compromission. Ces mesures sont définies dans les documents de planification ou de mission pertinents.

5. Des visites d'évaluation dans des pays tiers ou des organisations internationales, telles que visées à l'article 17 de la présente décision, sont organisées afin de garantir l'efficacité des mesures de sécurité en place en matière de protection de toute ICUE échangée.

6. La décision de communiquer des ICUE détenues par le SEAE à un pays tiers ou à une organisation internationale est prise au cas par cas, en fonction de la nature et du contenu de ces informations, du besoin d'en connaître du destinataire et d'une appréciation des avantages que l'UE peut en retirer.

Le SEAE demande le consentement écrit de toute entité ayant fourni des informations classifiées en tant que sources d'ICUE émanant du SEAE afin d'établir l'absence d'objection à leur communication.

Si l'autorité d'origine des informations classifiées à communiquer n'est pas le SEAE, le SEAE demande au préalable le consentement écrit de l'autorité d'origine.

Si, toutefois, le SEAE est dans l'impossibilité de déterminer l'autorité d'origine, l'autorité de sécurité du SEAE endosse la responsabilité de l'autorité d'origine après avoir obtenu l'avis unanimement favorable des États membres représentés au sein du comité de sécurité du SEAE.

7. Les modalités d'application du présent article figurent à l'annexe A VI.

Article 11

Infractions à la sécurité et compromission d'informations classifiées

1. Toute infraction à la sécurité, réelle ou présumée, et toute compromission d'informations classifiées, réelle ou présumée, sont immédiatement signalées à la direction du SEAE chargée de la sécurité, qui en informe, selon le cas, le ou les États membre(s) concerné(s), ou toute autre entité concernée.

2. Lorsqu'il est avéré ou qu'il existe des motifs raisonnables de supposer que des informations classifiées ont été compromises ou perdues, la direction du SEAE chargée de la sécurité en informe l'ANS du ou des États membres concernés et prend toutes les mesures nécessaires conformément aux dispositions législatives et réglementaires applicables afin:

a) de protéger les éléments de preuve;

b) de faire en sorte qu'une enquête soit menée par des membres du personnel n'étant pas directement concernés par l'infraction ou la compromission afin d'établir les faits;

c) d'informer immédiatement l'autorité d'origine ou toute autre entité concernée;

d) d'éviter que les faits ne se reproduisent;

e) d'évaluer le préjudice éventuel causé aux intérêts de l'UE ou des États membres; et

f) de notifier aux autorités concernées les effets de la compromission réelle ou présumée et des mesures prises.

3. Tout membre du personnel sous la responsabilité du SEAE qui enfreint les règles de sécurité énoncées dans la présente décision est passible d'une sanction disciplinaire conformément aux dispositions législatives et réglementaires applicables.

Toute personne responsable de la compromission ou de la perte d'informations classifiées est passible de sanctions disciplinaires et/ou peut faire l'objet d'une action en justice conformément aux dispositions législatives et réglementaires applicables.

4. Pendant que l'infraction et/ou la compromission font l'objet d'une enquête, le chef de la direction du SEAE chargée de la sécurité peut suspendre l'accès individuel aux ICUE et aux locaux du SEAE. La direction de la sécurité de la direction générale des ressources humaines et de la sécurité de la Commission, le bureau de sécurité du Secrétariat général du Conseil ou l'ANS du ou des États membres concernés, ou toute entité concernée, sont immédiatement informés de la présente décision.

ANNEXE A I

MESURES DE SÉCURITÉ CONCERNANT LE PERSONNEL

I. INTRODUCTION

1. La présente annexe contient les dispositions d'application de l'article 5 de l'annexe A. Elle prévoit les critères permettant au SEAE de déterminer si une personne, compte tenu de sa loyauté, de son intégrité et de sa fiabilité, peut être autorisée à avoir accès à des ICUE, ainsi que les procédures d'enquête et administratives à suivre à cet effet.

2. L'«habilitation de sécurité du personnel» (HSP) donnant accès aux ICUE, une autorisation émanant de l'autorité investie du pouvoir de nomination du SGC conformément à la présente décision à la suite d'une enquête de sécurité menée par les autorités compétentes d'un État membre et attestant qu'une personne peut, pour autant que son besoin d'en connaître ait été établi, être autorisée à avoir accès aux ICUE jusqu'à un niveau de classification donné (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur) jusqu'à une date donnée; la personne ainsi décrite est «habilitée».

3. Le «certificat d'habilitation de sécurité du personnel» (CHSP) est un certificat délivré par l'autorité de sécurité du SEAE précisant l'habilitation d'une personne et le niveau de classification des ICUE auxquelles l'intéressé peut se voir accorder l'accès, la date de validité de la HSP concernée et la date d'expiration du certificat lui-même.

4. L'«autorisation d'accès aux ICUE» est une autorisation que prend l'autorité de sécurité du SEAE en conformité avec la présente décision après qu'une HSP a été délivrée par les autorités compétentes d'un État membre, attestant qu'une personne peut, pour autant que son besoin d'en connaître ait été établi, être autorisée à avoir accès aux ICUE jusqu'à un niveau de classification donné (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur) jusqu'à une date donnée; la personne ainsi décrite est «habilitée».

II. AUTORISER L'ACCÈS AUX ICUE

5. L'accès à des informations classifiées RESTREINT UE/EU RESTRICTED ne nécessite pas d'habilitation de sécurité et est accordé après:

   a) établissement du lien statutaire ou contractuel de la personne concernée avec le SEAE;

   b) détermination du besoin d'en connaître de la personne;

   c) notification des règles et procédures de sécurité applicables à la protection des ICUE et reconnaissance écrite des responsabilités qui lui incombent en matière de protection de ces informations conformément à la présente décision.

6. Une personne ne peut être autorisée à avoir accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur qu'après:

   a) établissement du lien statutaire ou contractuel de la personne concernée avec le SEAE;

   b) que son besoin d'en connaître a été établi;

   c) s'être vu accorder une HSP du niveau correspondant ou avoir été dûment autorisée en vertu de ses fonctions conformément aux dispositions législatives et réglementaires nationales; et

   d) avoir été informée des règles et procédures de sécurité applicables à la protection des ICUE et avoir reconnu par écrit les responsabilités qui lui incombent en matière de protection de ces informations.

7. Le SEAE répertorie, au sein de ses structures, les postes nécessitant l'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur et exigeant par conséquent une HSP du niveau correspondant, conformément au paragraphe 4 ci-dessus.

8. Les membres du personnel du SEAE déclarent s'ils possèdent la nationalité de plusieurs pays.

Procédures de demande d'HSP au sein du SEAE

9. En ce qui concerne les membres du personnel du SEAE, l'autorité de sécurité du SEAE transmet le questionnaire de sécurité du personnel rempli à l'ANS de l'État membre dont l'intéressé est ressortissant et demande qu'il soit procédé à une enquête de sécurité pour le niveau de classification des ICUE auxquelles l'intéressé devra avoir accès.

10. Lorsqu'une personne possède la nationalité de plusieurs pays, la demande d'enquête de sécurité est adressée à l'ANS du pays dont la personne recrutée est ressortissante.

11. Si des informations utiles à une enquête de sécurité sont portées à la connaissance du SEAE concernant une personne ayant demandé une HSP, le SEAE, agissant conformément à la réglementation applicable, en avertit l'ANS compétente.

12. À l'issue de l'enquête de sécurité, l'ANS compétente notifie à la direction du SEAE chargée de la sécurité les conclusions de l'enquête en question.

    a) Lorsque, à l'issue de l'enquête de sécurité, on obtient l'assurance qu'il n'existe pas de renseignements défavorables de nature à mettre en doute la loyauté, l'intégrité et la fiabilité de l'intéressé, l'autorité de sécurité du SEAE peut accorder à l'intéressé une autorisation d'accès à des ICUE du niveau de classification correspondant jusqu'à une date déterminée.

    b) Le SEAE prend toutes les mesures qui s'imposent pour veiller à ce que les conditions ou restrictions imposées par l'ANS soient dûment mises en œuvre. L'ANS est informée des résultats.

    c) Lorsque, à l'issue de l'enquête de sécurité, on n'obtient pas cette assurance, l'autorité de sécurité du SEAE en informe l'intéressé, qui peut demander à être entendu par l'autorité de sécurité du SEAE. Celle-ci peut demander à l'ANS compétente tout éclaircissement complémentaire qu'elle est en mesure de donner conformément à ses dispositions législatives et réglementaires nationales. En cas de confirmation des résultats, l'autorisation d'accès aux ICUE n'est pas accordée. Dans ce cas, le SEAE prend toutes les mesures qui s'imposent pour que le demandeur se voie refuser tout accès aux ICUE.

13. L'enquête de sécurité et ses résultats, sur lesquels le SEAE fonde sa décision d'octroi ou de refus d'une autorisation d'accès aux ICUE, obéissent aux dispositions législatives et réglementaires en vigueur dans l'État membre concerné, y compris celles relatives aux recours. Les décisions de l'autorité de sécurité du SEAE sont susceptibles de recours conformément au statut.

14. L'assurance sur laquelle une HSP se fonde, pour autant qu'elle reste valable, couvre toute fonction exercée par l'intéressé au sein du SEAE, du Secrétariat général du Conseil ou de la Commission.

15. Le SEAE acceptera l'autorisation d'accès à des ICUE octroyée par toute autre institution, organe ou agence de l'Union européenne, pour autant qu'elle reste valable. Les autorisations couvriront toute fonction exercée par l'intéressé au sein du SEAE. L'institution, l'organe ou l'agence de l'Union européenne dans lequel la personne prend ses fonctions signalera le changement d'employeur à l'ANS concernée.

16. Si l'intéressé n'entame pas sa période de service dans un délai de douze mois à compter de la notification des conclusions de l'enquête de sécurité à l'autorité de sécurité du SEAE ou si cette période de service connaît une interruption d'au moins douze mois au cours de laquelle l'intéressé n'occupe pas de poste au sein du SEAE, d'autres institutions, organes ou organismes de l'UE, ou d'une administration nationale d'un État membre nécessitant un accès à des informations classifiées, les conclusions précitées sont soumises à l'ANS compétente afin que celle-ci confirme qu'elles restent valables et pertinentes.

17. Si des informations sont portées à la connaissance du SEAE concernant un risque de sécurité que représente une personne titulaire d'une HSP valide, le SEAE, agissant conformément à la réglementation applicable, en avertit l'ANS compétente et peut suspendre l'accès aux ICUE ou retirer l'autorisation d'accès à des ICUE. Lorsqu'une ANS notifie au SEAE que l'assurance visée au paragraphe 12, point a), est retirée à une personne titulaire d'une autorisation d'accès aux ICUE valide, l'autorité de sécurité du SEAE peut demander à l'ANS concernée tout éclaircissement qu'elle est en mesure de donner dans le respect de ses dispositions législatives et réglementaires nationales. Si les informations défavorables sont confirmées, l'autorisation susmentionnée est retirée et la personne concernée n'est plus autorisée à avoir accès aux ICUE, ni à des postes où un tel accès est possible et où elle pourrait nuire à la sécurité.

18. Toute décision de retirer une autorisation d'accès aux ICUE à un membre du personnel du SEAE et, s'il y a lieu, les raisons la justifiant sont communiquées à la personne concernée, qui peut demander à être entendue par l'autorité de sécurité du SEAE. Les informations communiquées par une ANS sont soumises aux dispositions législatives et réglementaires en vigueur dans l'État membre concerné, y compris celles relatives aux recours. Les décisions de l'autorité de sécurité du SEAE sont susceptibles de recours conformément au statut.

19. Les experts nationaux détachés auprès du SEAE pour occuper un poste nécessitant un accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur doivent présenter à l'autorité de sécurité du SEAE avant de prendre leurs fonctions une HSP valable leur donnant accès aux ICUE. La procédure susmentionnée est gérée par l'État membre qui détache les experts nationaux.

Registres des HSP

20. Une base de données pour l'état d'habilitation, en matière de sécurité, de tous les membres du personnel placés sous la responsabilité du SEAE et de ses contractants est administrée par le SEAE. Ces registres contiennent le niveau de classification des ICUE auxquelles l'intéressé peut se voir accorder l'accès (CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau supérieur), la date à laquelle l'HSP a été délivrée et sa durée de validité.

21. Des procédures de coordination adéquates sont mises en place avec les États membres et d'autres institutions, organes et organismes de l'UE pour faire en sorte que le SEAE tienne des registres précis et complets concernant l'état de l'habilitation de sécurité de tous les membres du personnel placés sous la responsabilité du SEAE et des effectifs de ses contractants.

22. L'autorité de sécurité du SEAE peut délivrer un certificat d'habilitation de sécurité du personnel (CHSP) précisant le niveau de classification des ICUE auxquelles l'intéressé peut se voir accorder l'accès (CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau supérieur), la durée de validité de l'HSP ou de l'autorisation, et la date d'expiration du certificat proprement dit.

Exemptions de l'obligation d'HSP

23. Les personnes dûment autorisées à accéder aux ICUE de par les fonctions qu'elles exercent, conformément aux dispositions législatives et réglementaires nationales, sont informées, le cas échéant, par la direction du SEAE chargée de la sécurité des obligations qui leur incombent pour la sécurité des ICUE.

III. FORMATION ET SENSIBILISATION À LA SÉCURITÉ

24. Avant d'être autorisées à accéder aux ICUE, toutes les personnes reconnaissent par écrit qu'elles ont bien compris leurs obligations en matière de protection des ICUE et des conséquences qui pourraient résulter si des ICUE devaient être compromises. Le SEAE tient un registre de ces déclarations écrites.

25. Toutes les personnes autorisées à avoir accès aux ICUE ou tenues de les traiter sont averties dans un premier temps et périodiquement informées par la suite des menaces pesant sur la sécurité, et elles doivent rendre compte immédiatement aux autorités de sécurité compétentes de toute démarche ou activité qu'elles jugent suspecte ou inhabituelle.

26. Toutes les personnes ayant accès aux ICUE sont constamment soumises aux mesures de sécurité du personnel permanentes (c'est-à-dire assistance) pendant qu'elles traitent des ICUE. La sécurité permanente du personnel incombe:

    a) aux personnes autorisées à accéder aux ICUE: les intéressés sont personnellement responsables de leur propre comportement en matière de sécurité et doivent signaler immédiatement aux autorités de sécurité compétentes toute démarche ou activité qu'ils jugent suspecte ou inhabituelle, ainsi que toute modification de leur propre situation personnelle qui pourrait avoir une incidence sur leur HSP ou autorisation d'accéder aux ICUE;

    b) aux supérieurs hiérarchiques: ils sont tenus de veiller à ce que leur personnel soit bien au courant des mesures de sécurité et des responsabilités quant à la protection des ICUE, de contrôler la conduite des membres du personnel quant à la sécurité et soit de traiter eux-mêmes tout problème de sécurité, soit de relayer aux autorités de sécurité compétentes toute information négative susceptible d'avoir une incidence sur l'HSP ou l'autorisation d'accéder aux ICUE des membres de leur personnel;

c) aux intervenants en matière de sécurité de l'organisation de la sécurité du SEAE telle que visée à l'article 12 de la présente décision: ils sont tenus de proposer des mises au point en matière de sécurité afin que les membres du personnel relevant de leur domaine bénéficient d'informations régulières, de promouvoir une culture de sécurité solide dans leur domaine de responsabilité, de mettre en place des mesures de contrôle de la conduite des membres du personnel en matière de sécurité, ainsi que de signaler aux autorités de sécurité compétentes toute information négative qui pourrait avoir une incidence sur les HSP de toute personne;

d) au SEAE et aux États membres: ils mettent en place les nécessaires canaux de communication d'informations susceptibles d'avoir une incidence sur l'HSP ou autorisation d'accéder aux ICUE de toute personne.

27. Toutes les personnes qui cessent d'exercer des fonctions nécessitant un accès aux ICUE sont informées, et le cas échéant reconnaissent par écrit, qu'elles ont l'obligation de continuer à protéger les ICUE.

IV. CIRCONSTANCES EXCEPTIONNELLES

28. En cas d'urgence, lorsque cela est dûment justifié dans l'intérêt du SEAE et en attendant l'achèvement de l'enquête de sécurité complète, l'autorité de sécurité du SEAE peut, après avoir consulté l'ANS de l'État membre dont l'intéressé est ressortissant et sous réserve des résultats des vérifications préliminaires effectuées pour s'assurer de l'absence d'informations défavorables, accorder à titre temporaire aux fonctionnaires et autres agents du SEAE l'autorisation d'accéder à des ICUE pour une fonction déterminée. Une enquête de sécurité complète doit être réalisée le plus rapidement possible. Ces autorisations temporaires seront valables pour une période ne dépassant pas six mois et ne donnent pas accès aux informations classifiées TRÈS SECRET UE/EU TOP SECRET. Toutes les personnes auxquelles a été délivrée une autorisation temporaire reconnaissent par écrit qu'elles ont bien compris leurs obligations en matière de protection des ICUE et les conséquences qui pourraient résulter si des ICUE devaient être compromises. Le SEAE tient un registre de ces déclarations écrites.

29. Lorsqu'une personne doit être affectée à un poste requérant une HSP dont le niveau dépasse d'un niveau celui qu'elle possède, l'affectation peut être décidée à titre provisoire, pour autant que les conditions suivantes soient réunies:

a) l'accès aux ICUE d'un niveau supérieur répond à une nécessité impérieuse qui doit être justifiée par écrit par le supérieur hiérarchique de la personne concernée;

b) l'accès doit être limité à des éléments particuliers des ICUE et servir aux attributions;

c) l'intéressé possède une HSP valide;

d) des démarches ont été entreprises en vue d'obtenir une autorisation pour le niveau d'accès nécessaire pour le poste;

e) des contrôles satisfaisants ont été effectués par l'autorité compétente permettant d'établir l'absence de violations graves ou répétées du règlement de sécurité par la personne concernée;

f) l'affectation de la personne est approuvée par l'autorité du SEAE compétente;

g) l'ANS/ASD compétente qui a délivré l'HSP à l'intéressé a été consultée et aucune objection n'a été formulée; et

h) une trace de l'accès exceptionnel, y compris une description des informations auxquelles l'accès a été donné, est conservée par le bureau d'ordre ou le bureau d'ordre subordonné compétent.

30. La procédure décrite ci-dessus est utilisée pour un accès ponctuel à des ICUE dont la classification dépasse d'un niveau le niveau d'habilitation de la personne concernée. Il ne convient pas de recourir de manière répétée à cette procédure.

31. Dans des circonstances très exceptionnelles, c'est-à-dire en cas de missions dans un environnement hostile ou au cours de périodes de tension internationale croissante lorsque des mesures d'urgence l'exigent, plus particulièrement afin de sauver des vies, la HR, l'autorité de sécurité du SEAE ou la DGBA peuvent accorder, si possible par écrit, un accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET à des personnes qui ne détiennent pas l'HSP requise, à condition que l'accès accordé soit absolument indispensable. Une trace de l'autorisation précisant les informations pour lesquelles l'accès a été approuvé doit être conservée.

32. Pour les informations classifiées TRÈS SECRET UE/EU TOP SECRET, un tel accès d'urgence est limité aux ressortissants d'États membres de l'UE s'étant vu octroyer l'accès soit à des informations dont le niveau de classification national équivaut à TRÈS SECRET UE/EU TOP SECRET soit à des informations classifiées SECRET UE/EU SECRET.

33. Le comité de sécurité du SEAE est informé des cas où il est recouru à la procédure décrite aux paragraphes 31 et 32.

34. Chaque année, le comité de sécurité du SEAE reçoit un rapport sur le recours aux procédures énoncées dans la présente section.

V. PARTICIPATION AUX RÉUNIONS AU SIÈGE DU SEAE ET DANS LES DÉLÉGATIONS DE L'UNION

35. Les personnes désignées pour participer à des réunions au siège du SEAE et dans les délégations de l'Union au sein desquelles des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont traitées ne peuvent le faire qu'après confirmation de la situation de l'intéressé au regard de l'HSP. Pour les représentants des États membres, les fonctionnaires du SCG et de la Commission, un CHSP ou toute autre preuve d'HSP est transmis par les autorités concernées à la direction du SEAE chargée de la sécurité, au coordinateur de la sécurité de la délégation de l'Union ou, à titre exceptionnel, est présenté par l'intéressé. Le cas échéant, il peut être fait usage d'une liste de noms récapitulative mentionnant les preuves d'habilitation voulues.

36. Lorsqu'une HSP permettant d'accéder à des ICUE est retirée à une personne dont la fonction l'oblige à participer à des réunions au siège du SEAE ou dans une délégation de l'Union auxquelles des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont traitées, le SEAE en est informé par l'autorité compétente.

VI. ACCÈS POTENTIEL AUX ICUE

37. Lorsqu'une personne doit être employée dans une fonction susceptible de lui donner un accès potentiel à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau supérieur, elle doit être dûment habilitée ou escortée en permanence.

38. Les courriers, les gardes et les escortes doivent disposer d'une habilitation de sécurité du niveau correspondant ou faire l'objet d'une enquête appropriée conformément aux dispositions législatives et réglementaires nationales, et être informés à intervalles réguliers des procédures de sécurité applicables à la protection des ICUE ainsi que des obligations qui leur incombent en matière de protection des informations de cette nature qui leur sont confiées ou auxquelles ils peuvent avoir accès par inadvertance.

ANNEXE A II

SÉCURITÉ PHYSIQUE DES INFORMATIONS CLASSIFIÉES DE L'UE

I. INTRODUCTION

1. La présente annexe contient les dispositions d'application de l'article 6 de l'annexe A. Elle énonce les règles minimales de protection physique des locaux, bâtiments, bureaux, salles et autres zones où des ICUE sont traitées et stockées, y compris des zones hébergeant des SIC.

2. Les mesures de sécurité physique sont destinées à prévenir l'accès non autorisé aux ICUE:

   a) en garantissant que les ICUE sont correctement traitées et stockées;

   b) en permettant d'établir une distinction entre les membres du personnel au regard de l'accès aux ICUE sur la base de leur besoin d'en connaître et, le cas échéant, de leur habilitation de sécurité;

   c) en ayant un effet dissuasif, en empêchant et en détectant les actes non autorisés; et

   d) en empêchant ou en retardant toute intrusion par la ruse ou par la force.

II. RÈGLES ET MESURES EN MATIÈRE DE SÉCURITÉ PHYSIQUE

3. Il convient que le SEAE applique une procédure de gestion des risques pour protéger les ICUE dans leurs locaux afin de garantir un niveau de protection physique qui soit proportionné au risque évalué. La procédure de gestion des risques tient compte de tous les facteurs pertinents, et notamment:

   a) du niveau de classification des ICUE;

   b) de la forme et du volume des ICUE, sachant que l'application de mesures de protection plus strictes pourrait être requise pour des volumes importants ou en cas de compilation d'ICUE;

   c) de l'environnement et de la structure des bâtiments ou des zones où se trouvent des ICUE;

   d) des évaluations de la menace de pays tiers telles qu'élaborées par INTCEN sur la base, en particulier, de rapports établis par les délégations de l'Union; et

   e) de l'évaluation de la menace que constituent les services de renseignement prenant pour cible l'UE ou des États membres, ainsi que les actes de sabotage, le terrorisme et les activités subversives ou les autres activités criminelles.

4. En appliquant la notion de défense en profondeur, l'autorité de sécurité du SEAE détermine la bonne combinaison de mesures de sécurité physique qu'il convient de mettre en œuvre. Il peut s'agir d'une ou de plusieurs des mesures suivantes:

   a) barrière périmétrique: une barrière physique qui défend les limites d'une zone devant être protégée;

   b) système de détection des intrusions (SDI): un tel système peut être utilisé pour améliorer le niveau de sécurité d'une barrière périmétrique ou dans des salles et des bâtiments pour remplacer le personnel de sécurité ou l'aider dans sa tâche;

   c) contrôle des accès: il peut être exercé sur un site, un ou plusieurs bâtiments d'un site ou des zones ou salles à l'intérieur d'un bâtiment. Ce contrôle peut être exercé par des moyens électroniques ou électromécaniques, par un membre du personnel de sécurité et/ou un réceptionniste, ou par tout autre moyen physique;

   d) personnel de sécurité: un personnel de sécurité formé, supervisé et, au besoin, dûment habilité peut être employé, notamment, pour dissuader des personnes de planifier des intrusions clandestines;

   e) système de télévision en circuit fermé (CCTV): un tel système peut être utilisé par le personnel de sécurité pour effectuer des vérifications en cas d'incident ou de déclenchement de l'alarme des SDI sur des sites étendus ou des enceintes;

f) éclairage de sécurité: un tel éclairage peut être utilisé pour dissuader un intrus potentiel ainsi que pour fournir la lumière nécessaire à une surveillance efficace, soit directement par le personnel de sécurité soit indirectement par l'intermédiaire d'un système de CCTV; et

g) toute autre mesure physique appropriée destinée à avoir un effet dissuasif quant à l'accès non autorisé ou à détecter un tel accès, ou à prévenir la perte ou la détérioration d'ICUE.

5. La direction du SEAE chargée de la sécurité peut mener des fouilles aux entrées et aux sorties afin d'avoir un effet dissuasif quant à l'introduction non autorisée de matériel dans des locaux ou des bâtiments ou au retrait non autorisé de toute ICUE des lieux précités.

6. Lorsque des ICUE risquent d'être vues, même accidentellement, des mesures appropriées sont prises pour parer à ce risque.

7. Pour les nouveaux établissements, les règles en matière de sécurité physique et leurs spécifications fonctionnelles doivent être définies lors de la planification et de la conception des établissements. Pour les établissements existants, les règles en matière de sécurité physique doivent être appliquées dans toute la mesure du possible.

III. ÉQUIPEMENT DESTINÉ À LA PROTECTION PHYSIQUE DES ICUE

8. Lors de l'achat de l'équipement destiné à la protection physique des ICUE (comme des meubles de sécurité, des déchiqueteuses, des serrures de porte, des systèmes électroniques de contrôle des accès, des SDI, des systèmes d'alarme), l'autorité de sécurité du SEAE veille à ce que cet équipement réponde aux normes techniques et aux conditions minimales agréées.

9. Les spécifications techniques de l'équipement devant servir à la protection physique des ICUE sont définies dans des lignes directrices en matière de sécurité, qu'il appartient au comité de sécurité du SEAE d'approuver.

10. Les systèmes de sécurité sont périodiquement inspectés et l'équipement est entretenu à intervalles réguliers. L'entretien prend en compte les résultats des inspections afin de garantir un fonctionnement optimal continu de l'équipement.

11. Il convient de réévaluer à chaque inspection l'efficacité des différentes mesures de sécurité et du système de sécurité dans son ensemble.

IV. ZONES PHYSIQUEMENT PROTÉGÉES

12. Deux types de zones physiquement protégées, ou leurs équivalents au niveau national, sont créés en vue de la protection physique des ICUE:

a) les zones administratives et

b) les zones sécurisées (dont les zones sécurisées du point de vue technique).

13. Il appartient à l'autorité de sécurité du SEAE d'établir qu'une zone répond aux conditions requises pour être désignée comme zone administrative, zone sécurisée ou zone sécurisée du point de vue technique.

14. Pour les zones administratives:

a) un périmètre défini est établi de façon visible afin de permettre le contrôle des personnes et, dans la mesure du possible, des véhicules;

b) ne peuvent y pénétrer sans escorte que les personnes dûment autorisées par la direction du SEAE chargée de la sécurité; et

c) toutes les autres personnes sont escortées en permanence ou font l'objet de contrôles équivalents.

15. Pour les zones sécurisées:

a) un périmètre défini et protégé est établi de façon visible et toutes les entrées et sorties sont contrôlées par un système de laissez-passer ou d'identification individuelle;

b) ne peuvent y pénétrer sans escorte que les personnes habilitées au niveau adéquat et expressément autorisées à y entrer sur la base de leur besoin d'en connaître;

c) toutes les autres personnes sont escortées en permanence ou font l'objet de contrôles équivalents.

16. Lorsque le fait de pénétrer dans une zone sécurisée équivaut en pratique à un accès direct aux informations classifiées qu'elle renferme, les règles supplémentaires suivantes sont d'application:

a) le niveau de classification le plus élevé qui s'applique aux informations conservées habituellement dans la zone doit être clairement indiqué;

b) tous les visiteurs doivent disposer d'une autorisation spécifique pour pénétrer dans la zone, sont escortés en permanence et disposent de l'habilitation de sécurité correspondante, sauf si des mesures sont prises pour empêcher l'accès aux ICUE;

c) les appareils électroniques sont laissés hors de la zone.

17. Les zones sécurisées qui sont protégées contre les écoutes sont qualifiées de zones sécurisées du point de vue technique. Les règles supplémentaires suivantes sont applicables:

a) ces zones sont équipées de SDI, verrouillées lorsqu'elles ne sont pas occupées et gardées lorsqu'elles sont occupées. Toutes les clés sont contrôlées conformément à la section VI de la présente annexe;

b) toutes les personnes et tous les matériels entrant dans ces zones sont contrôlés;

c) ces zones doivent faire l'objet, à intervalles réguliers, d'inspections physiques et/ou techniques selon les exigences de l'autorité de sécurité du SEAE. Ces inspections doivent également être effectuées après une entrée non autorisée, réelle ou présumée; et

d) ces zones ne sont pas équipées de lignes de communication, de téléphones ou d'autres dispositifs de communication ou matériels électriques ou électroniques qui ne sont pas autorisés;

18. Nonobstant le paragraphe 17, point d), avant d'être utilisé dans des zones dans lesquelles sont organisées des réunions ou sont exécutées des tâches mettant en jeu des informations classifiées SECRET UE/EU SECRET et d'un niveau de classification supérieur, et lorsque la menace pesant sur des ICUE est jugée élevée, tout dispositif de communication et tout matériel électrique ou électronique est d'abord examiné par l'autorité de sécurité du SEAE pour vérifier qu'aucune information intelligible ne peut être transmise par inadvertance ou de manière illicite par ces équipements en dehors du périmètre de la zone sécurisée.

19. Les zones sécurisées qui ne sont pas occupées vingt-quatre heures sur vingt-quatre par le personnel de service sont, au besoin, inspectées après les heures normales de travail et à intervalles aléatoires en dehors de ces heures, sauf si un SDI a été installé.

20. Des zones sécurisées et des zones sécurisées du point de vue technique peuvent être temporairement établies dans une zone administrative en vue de la tenue d'une réunion classifiée ou à toute autre fin similaire.

21. Des procédures d'exploitation de sécurité sont arrêtées pour chacune des zones sécurisées et précisent:

a) le niveau de classification des ICUE traitées ou stockées dans la zone;

b) les mesures de surveillance et de protection qu'il convient de mettre en place;

c) les personnes autorisées à pénétrer dans la zone en raison de leur besoin d'en connaître et en fonction de leur habilitation;

d) le cas échéant, les procédures applicables aux escortes ou à la protection des ICUE lorsque d'autres personnes sont autorisées à pénétrer dans la zone;

e) les autres mesures et procédures applicables.

22. Les chambres fortes sont installées dans des zones sécurisées. Les murs, les planchers, les plafonds, les fenêtres et les portes verrouillables sont approuvés par l'autorité de sécurité du SEAE et offrent une protection équivalente à celle d'un meuble de sécurité approuvé pour le stockage d'ICUE du même niveau de classification.

V. MESURES DE PROTECTION PHYSIQUES APPLICABLES AU TRAITEMENT ET AU STOCKAGE DES ICUE

23. Les ICUE classifiées RESTREINT UE/EU RESTRICTED peuvent être traitées:

a) dans une zone sécurisée;

b) dans une zone administrative à condition que les personnes non autorisées ne puissent avoir accès aux ICUE; ou

c) en dehors d'une zone sécurisée ou d'une zone administrative à condition que le détenteur les transporte conformément aux dispositions de l'annexe A III, paragraphes 30 à 42, et se soit engagé à se conformer aux mesures compensatoires prévues dans les instructions de sécurité émises par l'autorité de sécurité du SEAE pour empêcher que des personnes non autorisées aient accès aux ICUE.

24. Les ICUE classifiées RESTREINT UE/EU RESTRICTED sont stockées dans un meuble de bureau adapté et fermé dans une zone administrative ou dans une zone sécurisée. Ces informations peuvent être temporairement stockées en dehors d'une zone sécurisée ou d'une zone administrative à condition que le détenteur se soit engagé à se conformer aux mesures compensatoires prévues dans les instructions de sécurité émises par l'autorité de sécurité du SEAE.

25. Les ICUE classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET peuvent être traitées:

a) dans une zone sécurisée;

b) dans une zone administrative à condition que les personnes non autorisées ne puissent avoir accès aux ICUE; ou

c) en dehors d'une zone sécurisée ou d'une zone administrative à condition que le détenteur:

i) transporte les ICUE conformément aux dispositions de l'annexe A III, paragraphes 30 à 42;

ii) se soit engagé à se conformer aux mesures compensatoires prévues dans les instructions de sécurité émises par l'autorité de sécurité du SEAE pour empêcher que des personnes non autorisées aient accès aux ICUE;

iii) exerce en personne un contrôle permanent sur les ICUE; et

iv) si les documents sont sous forme papier, qu'il en ait informé le bureau d'ordre compétent.

26. Les ICUE classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET sont stockées dans une zone sécurisée, dans un meuble de sécurité ou une chambre forte.

27. Les ICUE classifiées TRÈS SECRET UE/EU TOP SECRET sont traitées dans une zone sécurisée.

28. Les ICUE classifiées TRÈS SECRET UE/TOP SECRET UE sont stockées dans une zone sécurisée, au siège selon l'une des modalités suivantes:

a) dans un meuble de sécurité conformément au paragraphe 8, moyennant un ou plusieurs des contrôles supplémentaires suivants:

i) protection ou vérification en permanence par un membre habilité du personnel de sécurité ou du personnel de service;

ii) système de détection des intrusions approuvé auquel on associe du personnel de sécurité prêt à intervenir en cas d'incident;

ou

b) dans une chambre forte équipée d'un système de détection des intrusions à laquelle on associe du personnel de sécurité prêt à intervenir en cas d'incident.

29. Les règles régissant le transport des ICUE en dehors des zones physiquement protégées figurent à l'annexe A III.

VI. CONTRÔLE DES CLÉS ET COMBINAISONS UTILISÉES POUR LA PROTECTION DES ICUE

30. L'autorité de sécurité du SEAE définit les procédures de gestion des clés et des combinaisons pour les bureaux, les salles, les chambres fortes et les meubles de sécurité. Ces procédures protègent d'un accès non autorisé.

31. Les combinaisons doivent être mémorisées par le plus petit nombre possible de personnes qui ont besoin de les connaître. Les combinaisons des meubles de sécurité et des chambres fortes servant au stockage d'ICUE doivent être changées:

    a) à la réception d'un nouveau meuble;

    b) lors de tout changement du personnel connaissant la combinaison;

    c) en cas de compromission, réelle ou présumée;

    d) lorsqu'une serrure a fait l'objet d'un entretien ou d'une réparation; et

    e) au moins tous les douze mois.

ANNEXE A III

GESTION DES INFORMATIONS CLASSIFIÉES

I. INTRODUCTION

1. La présente annexe contient les dispositions d'application de l'article 7 de l'annexe A. Elle prévoit les mesures administratives visant à contrôler les ICUE tout au long de leur cycle de vie en vue de contribuer à la dissuasion, à la détection et au retour aux conditions opérationnelles dans le cadre de la compromission ou de la perte délibérée ou accidentelle de telles informations.

II. GESTION DE LA CLASSIFICATION

Classifications et marquages

2. Les informations sont classifiées dans les cas où elles doivent être protégées compte tenu de leur confidentialité.

3. L'autorité d'origine des ICUE est chargée de déterminer le niveau de classification de sécurité, conformément aux lignes directrices applicables en matière de classification, et de diffuser les informations.

4. Le niveau de classification des ICUE est fixé conformément à l'article 2, paragraphe 2, de l'annexe A et en référence aux lignes directrices de sécurité qui doivent être approuvées conformément à l'article 3, paragraphe 3, de ladite annexe.

5. Les informations classifiées des États membres échangées avec le SEAE reçoivent le même niveau de protection que les ICUE portant une classification équivalente. Un tableau d'équivalence figure à l'appendice B de la présente décision.

6. La classification de sécurité et, le cas échéant, la date ou l'événement spécifique après laquelle ou lequel l'ICUE peut être déclassée ou déclassifiée seront indiqués clairement et correctement, que l'ICUE concernée soit au format papier, oral, électronique ou autre.

7. Les différentes parties d'un document donné (pages, paragraphes, sections, annexes, appendices et pièces jointes) peuvent nécessiter une classification différente et doivent alors porter le marquage afférent, y compris lorsqu'elles sont stockées sous forme électronique.

8. Dans la mesure du possible, les documents dont toutes les parties n'ont pas le même niveau de classification sont structurés de manière à ce que les parties ayant des niveaux de classification différents puissent au besoin être aisément identifiées et séparées des autres.

9. Le niveau général de classification d'un document ou d'un dossier est au moins aussi élevé que celui de sa partie portant la classification la plus élevée. Lorsqu'il rassemble des informations provenant de plusieurs sources, le document final est examiné pour en fixer le niveau général de classification de sécurité car il peut requérir un niveau de classification supérieur à celui de chacune des parties qui le composent.

10. Les lettres ou notes d'envoi accompagnant des pièces jointes portent le plus haut niveau de classification attribué à ces dernières. L'autorité d'origine indique clairement leur niveau de classification lorsqu'elles sont séparées de leurs pièces jointes, au moyen d'un marquage approprié, par exemple:

CONFIDENTIEL UE/EU CONFIDENTIAL

Sans pièce(s) jointe(s) RESTREINT UE/EU RESTRICTED

Marquages

11. Outre l'un des marquages de classification de sécurité prévus à l'article 2, paragraphe 2, de l'annexe A, les ICUE peuvent porter des marquages complémentaires, tels que:

a) un identifiant désignant l'autorité d'origine;

b) des marquages restrictifs, des mots-codes ou des acronymes utilisés pour préciser le domaine d'activité sur lequel porte le document ou pour indiquer une diffusion particulière en fonction du besoin d'en connaître ou des restrictions d'utilisation;

c) des marquages relatifs à la communicabilité.

12. Lorsqu'a été prise la décision de communiquer des ICUE à un pays tiers ou à une organisation internationale, la direction du SEAE chargée de la sécurité transmet les informations classifiées concernées, qui portent un marquage relatif à la communicabilité indiquant le pays tiers ou l'organisation internationale auquel ce document doit être communiqué.

13. Une liste des marquages autorisés est adoptée par l'autorité de sécurité du SEAE.

Abréviations indiquant la classification

14. Des abréviations uniformisées indiquant la classification peuvent être utilisées pour préciser le niveau de classification des différents paragraphes d'un texte. Les abréviations ne remplacent pas la mention de la classification en toutes lettres.

15. Les abréviations uniformisées ci-après peuvent être utilisées dans les documents classifiés de l'UE pour indiquer le niveau de classification de sections ou blocs de texte de moins d'une page:

TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE	S-UE/EU-S
CONFIDENTIEL EU/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Création d'ICUE

16. Lors de la création de documents classifiés de l'UE:

a) sur chaque page figure un marquage indiquant clairement le niveau de classification;

b) chaque page est numérotée;

c) le document porte un numéro de référence et un sujet qui n'est pas lui-même une information classifiée, sauf s'il s'est vu apposer un marquage à ce titre;

d) le document est daté;

e) les documents classifiés CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur portent un numéro d'exemplaire sur chaque page dès lors qu'ils doivent être diffusés en plusieurs exemplaires.

17. Lorsqu'il n'est pas possible d'appliquer le paragraphe 16 à des ICUE, d'autres mesures appropriées sont prises conformément aux lignes directrices en matière de sécurité qui doivent être arrêtées en vertu de la présente décision.

Déclassement et déclassification des ICUE

18. Au moment de la création du document classifié, l'autorité d'origine indique, si possible et notamment en ce qui concerne les informations classifiées RESTREINT UE/EU RESTRICTED, si les ICUE qui y figurent peuvent ou non être déclassées ou déclassifiées à une date donnée ou après un événement spécifique.

19. Le SEAE réexamine régulièrement les ICUE en sa possession pour déterminer si leur niveau de classification est toujours d'application. Le SEAE instaure un système pour réexaminer le niveau de classification des ICUE enregistrées dont il est l'auteur, au moins une fois tous les cinq ans. Un tel réexamen n'est pas nécessaire lorsque l'autorité d'origine a indiqué dès le départ que les informations seraient automatiquement déclassées ou déclassifiées à un moment précis et que celles-ci se sont vu apposer les marquages correspondants.

III. ENREGISTREMENT DES ICUE À DES FINS DE SÉCURITÉ

20. Un bureau d'ordre central est désigné au siège. Pour chacune des entités structurées qui existent au sein du SEAE et dans lesquelles des ICUE sont traitées, on détermine un bureau d'ordre compétent, subordonné au bureau d'ordre central, qui sera chargé de veiller à ce que les ICUE soient traitées conformément à la présente décision. Les bureaux d'ordre sont conçus comme des zones sécurisées telles que définies à l'annexe A.

Chaque délégation de l'Union instaure son propre bureau d'ordre responsable des ICUE.

L'autorité de sécurité du SEAE désigne un Chief Registry Officer pour ces bureaux d'ordre.

21. Aux fins de la présente décision, on entend par enregistrement à des fins de sécurité (ci-après «enregistrement») l'application de procédures permettant de garder la trace du cycle de vie d'une information, y compris de sa diffusion et de sa destruction. Dans le cas d'un SIC, les procédures d'enregistrement peuvent être mises en œuvre au moyen de processus intervenant au sein du SIC même.

22. Tout matériel classifié CONFIDENTIEL UE/EU CONFIDENTIAL et d'un niveau de classification supérieur est enregistré à chaque fois qu'il parvient à une entité structurée ou qu'il en sort, délégations de l'Union comprises. Les informations classifiées TRÈS SECRET UE/EU TOP SECRET sont enregistrées dans des bureaux d'ordre désignés.

23. Le bureau d'ordre central constitue, au siège du SEAE, le principal point d'entrée et de sortie pour les échanges d'informations classifiées avec des pays tiers et des organisations internationales. Il garde une trace de tous ces échanges.

24. L'autorité de sécurité du SEAE approuve des lignes directrices de sécurité concernant l'enregistrement des ICUE à des fins de sécurité, conformément à l'article 14 de la présente décision.

Bureaux d'ordre TRÈS SECRET UE/EU TOP SECRET

25. Un bureau d'ordre central est désigné au siège du SEAE pour faire fonction d'autorité centrale de réception et de diffusion des informations classifiées TRÈS SECRET UE/EU TOP SECRET. S'il y a lieu, des bureaux d'ordre subordonnés peuvent être désignés pour traiter ces informations à des fins d'enregistrement.

26. Ces bureaux d'ordre subordonnés ne peuvent pas transmettre de documents TRÈS SECRET UE/EU TOP SECRET directement à d'autres bureaux d'ordre subordonnés rattachés au même bureau d'ordre TRÈS SECRET UE/EU TOP SECRET central sans l'autorisation expresse et écrite de ce dernier ni à des bureaux d'ordre extérieurs.

IV. DUPLICATION ET TRADUCTION DES DOCUMENTS CLASSIFIÉS DE L'UE

27. Les documents classifiés TRÈS SECRET UE/EU TOP SECRET ne doivent pas être dupliqués ou traduits sans le consentement écrit préalable de l'autorité d'origine.

28. Lorsque l'autorité d'origine de documents classifiés SECRET UE/EU SECRET et d'un niveau de classification inférieur n'a pas imposé de restrictions à leur duplication ou à leur traduction, lesdits documents peuvent être dupliqués ou traduits sur instruction du détenteur.

29. Les mesures de sécurité applicables au document original le sont aussi à ses copies et à ses traductions. Les copies des informations CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont créées uniquement par le bureau d'ordre (subordonné) compétent au moyen d'un photocopieur sécurisé. Les copies doivent être enregistrées.

V. TRANSPORT DES ICUE

30. Le transport des ICUE est soumis aux mesures de protection énoncées aux paragraphes 32 à 42. Lorsque les ICUE sont transportées par des supports électroniques, et nonobstant l'article 7, paragraphe 4, de l'annexe A, les mesures de protection énoncées ci-après peuvent être complétées par des contre-mesures techniques appropriées prescrites par l'autorité de sécurité du SEAE, de façon à réduire au minimum le risque de perte ou de compromission.

31. L'autorité de sécurité du SEAE émet les instructions relatives au transport des ICUE conformément à la présente décision.

À l'intérieur d'un même bâtiment ou d'un groupe autonome de bâtiments

32. Les ICUE transportées à l'intérieur d'un même bâtiment ou d'un groupe autonome de bâtiments sont dissimulées en vue de prévenir l'observation de leur contenu.

33. À l'intérieur d'un bâtiment ou d'un groupe autonome de bâtiments, les informations classifiées TRÈS SECRET UE/EU TOP SECRET sont transportées par des membres du personnel disposant de l'habilitation de sécurité adéquate, dans une enveloppe sécurisée avec pour seule mention le nom du destinataire.

À l'intérieur de l'UE

34. Les ICUE transportées entre des bâtiments ou des locaux à l'intérieur de l'UE sont emballées de manière à être protégées de toute divulgation non autorisée.

35. Le transport d'informations classifiées jusqu'au niveau SECRET UE/EU SECRET à l'intérieur de l'UE s'effectue par l'un des moyens suivants:

    a) le courrier militaire, gouvernemental ou diplomatique, selon le cas;

    b) le transport par porteur, à condition:

        i) que le porteur ne se sépare pas des ICUE, à moins que leur stockage ne soit assuré conformément aux règles énoncées à l'annexe A II;

        ii) que les ICUE ne soit pas déballées pendant le transport ni lues dans des lieux publics;

        iii) que la personne soit habilitée au niveau adéquat et ait reçu des instructions quant à ses responsabilités en matière de sécurité;

        iv) que la personne soit, si nécessaire, munie d'un certificat de courrier;

    c) les services postaux ou les services de courrier commercial, à condition:

        i) qu'ils soient agréés par l'ANS compétente conformément aux dispositions législatives et réglementaires nationales;

        ii) qu'ils appliquent les mesures de protection appropriées conformément aux exigences minimales qui seront prévues dans les lignes directrices en matière de sécurité en vertu de l'article 21, paragraphe 1, de la présente décision.

    En cas de transport d'un État membre vers un autre État membre, les dispositions du point c) sont limitées aux informations classifiées jusqu'au niveau CONFIDENTIEL UE/EU CONFIDENTIAL.

36. Le matériel classifié CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET (par exemple, équipement ou machine) qui ne peut être transporté par les moyens visés au paragraphe 34 est transporté en tant que fret par des sociétés de transport commercial conformément à l'annexe A V.

37. Le transport des informations classifiées TRÈS SECRET UE/EU TOP SECRET, entre des bâtiments ou des locaux à l'intérieur de l'UE, s'effectue par courrier militaire, gouvernemental ou diplomatique, selon le cas.

De l'UE vers le territoire d'un pays tiers, ou entre des entités de l'UE situées dans des pays tiers

38. Les ICUE transportées de l'UE vers le territoire d'un pays tiers ou entre des entités de l'UE situées dans des pays tiers sont emballées de manière à être protégées de toute divulgation non autorisée.

39. Le transport des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET de l'UE vers le territoire d'un pays tiers et le transport des ICUE d'un niveau de classification allant jusqu'à SECRET UE/EU SECRET entre des entités de l'UE situées dans des pays tiers s'effectuent par l'un des moyens suivants:

    a) le courrier militaire ou diplomatique;

    b) le transport par porteur, à condition:

        i) que le paquet porte un sceau officiel ou soit emballé de manière à indiquer qu'il s'agit d'un envoi officiel ne devant pas être soumis à contrôle douanier ou de sécurité;

        ii) que la personne soit munie d'un certificat de courrier identifiant le paquet et l'autorisant à le transporter;

        iii) que le porteur ne se sépare pas des ICUE, à moins que leur stockage ne soit assuré conformément aux règles énoncées à l'annexe A II;

        iv) que les ICUE ne soit pas déballées pendant le transport ni lues dans des lieux publics; et

        v) que les personnes soient habilitées au niveau adéquat et aient reçu des instructions quant à leurs responsabilités en matière de sécurité.

40. Le transport des informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET communiquées par l'UE à un pays tiers ou à une organisation internationale est conforme aux dispositions applicables au titre d'un accord sur la sécurité des informations ou d'un arrangement administratif conclu en vertu de l'article 10, paragraphe 2, de l'annexe A.

41. Les informations classifiées RESTREINT UE/EU RESTRICTED peuvent aussi être transportées de l'UE vers le territoire d'un pays tiers par des services postaux ou par des services de courrier commercial.

42. Le transport des informations classifiées TRÈS SECRET UE/EU TOP SECRET de l'UE vers le territoire d'un pays tiers ou entre des entités de l'UE situées dans des pays tiers s'effectue par courrier militaire ou diplomatique.

VI. DESTRUCTION DES ICUE

43. Les documents classifiés de l'UE qui ne sont plus nécessaires peuvent être détruits, sans préjudice de la réglementation applicable en matière d'archivage.

44. Les documents faisant l'objet d'un enregistrement en application de l'article 7, paragraphe 2, de l'annexe A sont détruits par le bureau d'ordre compétent sur instruction du détenteur ou d'une autorité compétente. Les cahiers d'enregistrement et les autres informations relatives aux enregistrements sont actualisés en conséquence.

45. La destruction de documents classifiés SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET est effectuée en présence d'un témoin justifiant de l'habilitation de sécurité correspondant au moins au niveau de classification du document à détruire.

46. L'agent du bureau d'ordre et le témoin, lorsque la présence de ce dernier est requise, signent un procès-verbal de destruction qui est archivé dans le bureau d'ordre. Le bureau d'ordre conserve les procès-verbaux de destruction des documents TRÈS SECRET UE/EU TOP SECRET pendant dix ans au minimum, et ceux des documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET pendant cinq ans au minimum.

47. Les documents classifiés, y compris ceux dont la classification est RESTREINT UE/EU RESTRICTED, sont détruits par des méthodes répondant aux normes UE applicables ou à des normes équivalentes, ou homologuées par les États membres conformément aux normes techniques nationales, pour empêcher leur reconstitution totale ou partielle.

48. La destruction des supports de données informatiques utilisés pour des ICUE s'effectue conformément aux procédures approuvées par l'autorité de sécurité du SEAE.

VII. INSPECTIONS DE SÉCURITÉ

Inspections de sécurité du SEAE

49. En vertu de l'article 16 de la présente décision, les inspections de sécurité du SEAE englobent:

a) des inspections de sécurité générales, qui ont pour but d'évaluer le niveau de sécurité général du siège du SEAE, des délégations de l'Union et de tous les locaux dépendants ou connexes, en particulier afin d'évaluer l'efficacité des mesures de sécurité mises en œuvre aux fins de la protection des intérêts du SEAE à protéger;

b) des inspections de sécurité des ICUE, qui ont pour but d'évaluer, généralement aux fins d'une homologation, l'efficacité des mesures mises en œuvre aux fins de la protection des ICUE au sein du siège du SEAE et des délégations de l'Union.

Plus particulièrement, les inspections sont notamment menées aux fins suivantes:

i) veiller à ce que les normes minimales requises fixées dans la présente décision en matière de protection des ICUE soient respectées;

ii) mettre l'accent sur l'importance de la sécurité et d'une gestion efficace des risques au sein des entités inspectées;

iii) recommander des contre-mesures pour atténuer l'incidence particulière de la perte de confidentialité, d'intégrité ou de disponibilité des informations classifiées; et

iv) renforcer les programmes mis en place par les autorités de sécurité en matière de formation et de sensibilisation à la sécurité.

Conduite des inspections de sécurité du SEAE et comptes rendus y afférents

50. Les inspections de sécurité du SEAE sont conduites par une équipe d'inspection de la direction du SEAE chargée de la sécurité et, si nécessaire, avec l'aide d'experts en sécurité d'autres institutions de l'UE ou États membres.

L'équipe d'inspection a accès à tous les lieux, notamment aux bureaux d'ordre et aux points de présence SIC, où sont traitées des ICUE.

51. Les inspections de sécurité du SEAE dans les délégations de l'Union peuvent être conduites, si nécessaire, avec l'aide des responsables de la sécurité des ambassades des États membres situées dans les pays tiers.

52. L'autorité de sécurité du SEAE adopte, avant la fin de chaque année civile, le programme d'inspection du SEAE en matière de sécurité pour l'année suivante.

53. Des inspections de sécurité qui ne sont pas prévues au programme susmentionné peuvent, au besoin, être organisées par l'autorité de sécurité du SEAE.

54. À l'issue de l'inspection de sécurité, les principales conclusions et recommandations sont présentées à l'entité inspectée. Un rapport d'inspection est ensuite établi par l'équipe d'inspection. Lorsque des mesures correctives et des recommandations ont été proposées, le rapport doit contenir suffisamment d'éléments précis pour étayer les conclusions dégagées. Le rapport est transmis à l'autorité de sécurité du SEAE et au chef de l'entité inspectée.

Un rapport périodique est établi sous la responsabilité de la direction du SEAE chargée de la sécurité pour souligner les enseignements qui ont été tirés des inspections effectuées au cours d'une période précise et est examiné par le comité de sécurité du SEAE.

Conduite d'inspections de sécurité et comptes rendus y afférents dans les organes et organismes de l'UE établis en vertu du titre V, chapitre 2, du TUE

55. La direction du SEAE chargée de la sécurité peut, le cas échéant, désigner des experts qui apporteront leur contribution via leur participation aux équipes d'inspection conjointes de l'UE dans les organes et organismes de l'Union visés au titre V, chapitre 2, du traité sur l'Union européenne.

Liste de contrôle des inspections de sécurité du SEAE

56. La direction du SEAE chargée de la sécurité établit et met à jour une liste de contrôle des éléments à vérifier au cours d'une inspection de sécurité du SEAE. Cette liste de contrôle est transmise au comité de sécurité du SEAE.

57. Les informations nécessaires pour compléter la liste de contrôle sont obtenues, notamment au cours de l'inspection, auprès des services chargés de la gestion de la sécurité de l'entité faisant l'objet de l'inspection. Sitôt complétée avec les réponses détaillées obtenues, la liste de contrôle est classifiée en accord avec l'entité inspectée. Elle ne fait pas partie du rapport d'inspection.

ANNEXE A IV

PROTECTION DES ICUE TRAITÉES DANS LES SIC

I. INTRODUCTION

1. La présente annexe énonce les modalités d'application de l'article 8 de l'annexe A.

2. Les propriétés et les notions d'assurance de l'information (AI) définies ci-après sont essentielles pour la sécurité et l'exécution correcte des opérations dans le cadre de systèmes d'information et de communication (SIC):

Authenticité:	garantie que l'information est véridique et émane de sources dignes de foi;
Disponibilité:	caractéristique de l'information selon laquelle elle est accessible et utilisable, à la demande d'une entité autorisée;
Confidentialité:	propriété selon laquelle les informations ne sont pas divulguées à des personnes ou à des entités non autorisées et l'accès à ces informations n'est pas accordé à des processus non autorisés;
Intégrité:	propriété consistant à préserver l'exactitude et le caractère complet des informations et éléments;
Non-répudiation:	la possibilité de prouver qu'une action ou un événement a eu lieu, de sorte qu'il ne peut être contesté par la suite.

II. PRINCIPES D'ASSURANCE DE L'INFORMATION

3. Les dispositions énoncées ci-après constituent les éléments fondamentaux permettant de garantir la sécurité de tout SIC traitant des ICUE. Les modalités précises de mise en œuvre de ces dispositions sont définies dans les lignes directrices en matière de sécurité d'AI.

Gestion des risques de sécurité

4. La gestion des risques de sécurité fait partie intégrante de la définition, de l'élaboration, de l'exploitation et de la maintenance d'un SIC. La gestion des risques (évaluation, traitement, acceptation et communication) est mise en œuvre conjointement, dans le cadre d'un processus itératif, par les représentants des détenteurs de systèmes, les autorités responsables du projet, les autorités chargées de l'exploitation et les autorités d'homologation de sécurité selon une procédure d'évaluation des risques éprouvée, transparente et pouvant être parfaitement comprise. Le domaine d'application du SIC et ses ressources sont clairement définis dès le début du processus de gestion des risques.

5. Les autorités compétentes du SEAE examinent les menaces potentielles qui pèsent sur le SIC, tiennent à jour les évaluations des menaces et veillent à leur exactitude afin que celles-ci rendent compte de l'environnement opérationnel du moment. Elles actualisent en permanence leurs connaissances relatives aux questions de vulnérabilité et revoient régulièrement l'évaluation de la vulnérabilité afin de suivre l'évolution de la technologie de l'information.

6. La gestion des risques de sécurité vise à appliquer un ensemble de mesures de sécurité offrant un équilibre satisfaisant entre les besoins des utilisateurs et le risque de sécurité résiduel.

7. Les exigences spécifiques, l'étendue et le niveau de détail fixés par l'autorité d'homologation de sécurité (AHS) compétente aux fins de l'homologation d'un SIC sont proportionnés au risque évalué, compte tenu de tous les facteurs pertinents, y compris le niveau de classification des ICUE qui sont traitées dans le SIC. Dans le cadre de l'homologation, le risque résiduel fait l'objet d'un énoncé formel et est accepté par une autorité responsable.

Sécurité du SIC tout au long de son cycle de vie

8. Assurer la sécurité d'un SIC tout au long de son cycle de vie, de son lancement à son retrait, est une obligation.

9. Le rôle de chaque acteur d'un SIC et les interactions entre ces acteurs, en termes de sécurité du système, doivent être clairement déterminés pour chaque phase du cycle de vie.

10. Tout SIC, y compris les mesures de sécurité techniques et non techniques dont il fait l'objet, est soumis à des essais de sécurité au cours du processus d'homologation afin de s'assurer que le niveau d'assurance requis concernant les mesures de sécurité mises en œuvre est atteint et de vérifier qu'il est correctement mis en œuvre, intégré et configuré.

11. Des évaluations, inspections et examens de sécurité sont réalisés à intervalles réguliers durant la phase opérationnelle ainsi que dans le cadre de la maintenance d'un SIC, de même qu'en toute circonstance exceptionnelle.

12. Les documents relatifs à la sécurité d'un SIC évoluent tout au long du cycle de vie de celui-ci, évolution qui s'inscrit pleinement dans le cadre du processus de gestion du changement et de la configuration.

Meilleures pratiques

13. Le SEAE, le SCG, la Commission et les États membres travaillent de concert à l'élaboration des meilleures pratiques destinées à protéger les ICUE traitées par un SIC. Les lignes directrices concernant les meilleures pratiques énoncent des mesures visant à assurer la sécurité du SIC sur le plan technique et physique ainsi qu'au niveau de l'organisation et des procédures et dont l'efficacité pour lutter contre certaines menaces et vulnérabilités a été démontrée.

14. Il convient, aux fins de la protection des ICUE traitées par un SIC, de mettre à profit les enseignements tirés par les entités travaillant dans le domaine de l'AI, que ce soit au sein ou en dehors de l'UE.

15. La diffusion et la mise en œuvre ultérieure des meilleures pratiques contribuent à atteindre un niveau équivalent d'assurance dans les divers SIC traitant des ICUE exploités par le SEAE.

Défense en profondeur

16. Afin d'atténuer les risques qui pèsent sur un SIC, un éventail de mesures de sécurité techniques et non techniques organisées en plusieurs niveaux de défense doit être mis en œuvre. Ces niveaux sont notamment les suivants:

a) *dissuasion*: mesures de sécurité visant à dissuader un éventuel adversaire de projeter une attaque du SIC;

b) *prévention*: mesures de sécurité visant à empêcher ou à stopper une attaque du SIC;

c) *détection*: mesures de sécurité visant à déceler une attaque du SIC en train de se produire;

d) *résilience*: mesures de sécurité visant à faire en sorte que l'attaque n'ait une incidence que sur un nombre aussi faible que possible d'informations ou de ressources du SIC et à prévenir d'autres dommages; et

e) *rétablissement*: mesures de sécurité visant à rétablir la sécurité du SIC.

La rigueur et l'applicabilité de ces mesures de sécurité sont déterminées sur la base d'une évaluation des risques.

17. Les autorités compétentes du SEAE s'assurent qu'elles sont en mesure de faire face aux incidents dont l'ampleur dépasse les limites de l'organisation ou du pays touché, afin de coordonner les réactions et d'échanger des informations sur ces incidents et l'ensemble des risques qui en découlent (capacités de réaction en cas d'urgence informatique).

Principes du minimalisme et du moindre privilège

18. Seuls sont mis en œuvre les fonctions, dispositifs et services répondant aux exigences opérationnelles afin d'éviter tout risque inutile.

19. Les utilisateurs d'un SIC et les processus automatisés se voient uniquement accorder les droits d'accès, les privilèges ou les autorisations requises pour mener à bien leur tâche, afin de limiter tout dommage résultant d'accidents, d'erreurs ou d'utilisations non autorisées des ressources du SIC.

20. Les procédures d'enregistrement mises en œuvre par un SIC, le cas échéant, sont vérifiées dans le cadre du processus d'homologation.

Sensibilisation à l'assurance de l'information

21. La sensibilisation aux risques et aux mesures de sécurité disponibles constitue la première ligne de défense destinée à assurer la sécurité des SIC. En particulier, tout le personnel intervenant dans le cycle de vie d'un SIC, y compris les utilisateurs, doit bien comprendre:

    a) que les défaillances en matière de sécurité peuvent porter gravement atteinte aux SIC et à l'organisation dans son ensemble;

    b) le préjudice potentiel que peuvent causer à autrui l'interconnectivité et l'interdépendance; et

    c) la responsabilité et l'obligation de rendre des comptes qui lui incombent concernant la sécurité du SIC, selon les fonctions qui sont les siennes dans le cadre des systèmes et processus.

22. Afin que les responsabilités en matière de sécurité soient bien comprises, une formation et une sensibilisation à l'AI sont obligatoires pour tout le personnel concerné, y compris les cadres supérieurs et les utilisateurs du SIC.

Évaluation et approbation des produits de sécurité informatique

23. Le niveau de confiance requis dans les mesures de sécurité, défini comme un niveau d'assurance, est déterminé à l'issue du processus de gestion des risques et conformément aux politiques et lignes directrices applicables en matière de sécurité.

24. Le niveau d'assurance fait l'objet d'une vérification au moyen de procédés et de méthodes reconnus à l'échelon international ou agréés au niveau national. Il s'agit principalement d'évaluations, de contrôles et d'audits.

25. Les produits cryptographiques destinés à protéger les ICUE sont évalués et agréés par une autorité d'agrément cryptographique (AAC) nationale d'un État membre.

26. Avant d'être recommandés à l'AAC du SEAE pour agrément, en application de l'article 8, paragraphe 5, de la présente décision, ces produits cryptographiques doivent avoir satisfait à une évaluation par seconde partie réalisée par une autorité dûment qualifiée (AQUA) d'un État membre n'intervenant pas dans la conception ni dans la fabrication de l'équipement concerné. L'ampleur de l'évaluation par seconde partie nécessaire dépend du niveau de classification maximal envisagé des ICUE que ces produits doivent protéger.

27. Lorsque des motifs opérationnels particuliers le justifient, l'AAC du SEAE, selon le cas, peut, sur recommandation du comité de sécurité du Conseil, ne pas respecter les exigences prévues aux paragraphes 25 et 26 et délivrer un agrément à titre provisoire pour une période spécifique, en application de l'article 8, paragraphe 5, de la présente décision.

28. L'AQUA est une AAC d'un État membre qui a été agréée, sur la base de critères définis par le Conseil, pour procéder à la deuxième évaluation des produits cryptographiques destinés à protéger les ICUE.

29. La haute représentante approuve une politique de sécurité concernant la qualification et l'approbation des produits de sécurité informatique non cryptographiques.

Transmission à l'intérieur de zones sécurisées

30. Nonobstant les dispositions de la présente décision, lorsque la transmission d'ICUE s'effectue uniquement à l'intérieur de zones sécurisées ou de zones administratives, une transmission non chiffrée ou d'un niveau de chiffrement inférieur peut être envisagée compte tenu des résultats d'un processus de gestion des risques et avec l'accord de l'AHS.

Interconnexion sécurisée des SIC

31. Aux fins de la présente décision, on entend par «interconnexion» la connexion directe d'au moins deux systèmes informatiques permettant à ceux-ci d'échanger des données et d'autres ressources en matière d'information (communication, par exemple) de façon unidirectionnelle ou multidirectionnelle.

32. Un SIC doit de prime abord considérer tout système informatique interconnecté comme n'étant pas fiable et mettre en œuvre des mesures de protection destinées à contrôler les échanges d'informations classifiées.

33. Lorsqu'un SIC est interconnecté avec un autre système électronique, les conditions de base suivantes doivent être réunies:

    a) les conditions opérationnelles ou d'activités pour ces interconnexions sont définies et approuvées par les autorités compétentes;

    b) l'interconnexion est soumise à un processus de gestion des risques et d'homologation et est approuvée par les AHS compétentes; et

    c) des services de protection en bordure (SPB) sont mis en place à la périphérie de tout SIC.

34. Il ne peut y avoir aucune interconnexion entre un SIC homologué et un réseau non protégé ou public, sauf lorsque le SIC comporte un système de protection en bordure homologué installé à cette fin entre le SIC et le réseau non protégé ou public. Les mesures de sécurité applicables à une telle interconnexion sont examinées par l'autorité chargée de l'assurance de l'information (AAI) compétente et approuvées par l'AHS compétente.

    Lorsque le réseau public ou non protégé sert uniquement à des fins de transmission et que les données sont chiffrées au moyen d'un produit cryptographique agréé conformément à l'article 8, paragraphe 5, de la présente décision, une telle connexion n'est pas considérée comme une interconnexion.

35. Un SIC homologué pour traiter des informations TRÈS SECRET UE/EU TOP SECRET ne peut pas être interconnecté directement ou en cascade à un réseau non protégé ou public.

Supports de données informatiques

36. Les supports de données informatiques sont détruits conformément aux procédures approuvées par l'autorité de sécurité du SEAE.

37. Les supports de données informatiques sont réutilisés, déclassés ou déclassifiés conformément aux lignes directrices de sécurité arrêtées en vertu de l'article 8, paragraphe 2, de la présente décision.

Situations d'urgence

38. Nonobstant les dispositions de la présente décision, les procédures spécifiques décrites ci-après peuvent être appliquées, de manière limitée dans le temps, dans les situations d'urgence, telles que les crises, les conflits ou les guerres, imminents ou effectifs, ou dans des circonstances opérationnelles exceptionnelles.

39. Sous réserve du consentement de l'autorité compétente, les ICUE peuvent être transmises au moyen de produits cryptographiques agréés pour un niveau de classification inférieur ou sans faire l'objet d'un chiffrement dans le cas où tout retard causerait un préjudice indéniablement plus important que celui qui découlerait de la divulgation du matériel classifié et dans les conditions suivantes:

    a) l'expéditeur et le destinataire ne possèdent pas le dispositif de chiffrement nécessaire ou ne possèdent aucun dispositif de chiffrement; et

    b) le matériel classifié ne peut être communiqué en temps voulu par aucun autre moyen.

40. Les informations classifiées transmises dans les conditions visées au paragraphe 39 ne portent aucun marquage ni indication qui les distinguerait d'informations non classifiées ou pouvant être protégées à l'aide d'un produit cryptographique disponible. Leur destinataire est informé, sans délai et par d'autres moyens, du niveau de classification.

41. Lorsque le paragraphe 39 est invoqué, un rapport est par la suite adressé à la direction de la sécurité du SEAE, qui le communique à son tour au comité de sécurité du SEAE. Ledit rapport mentionne au moins l'expéditeur, le destinataire et l'autorité d'origine de chaque ICUE.

III. AUTORITÉS COMPÉTENTES EN MATIÈRE D'ASSURANCE DE L'INFORMATION

42. Les autorités compétentes en matière d'AI suivantes sont établies au sein du SEAE. Ces autorités ne doivent pas nécessairement être dotées d'entités structurées distinctes. Elles sont investies de mandats distincts. Cependant, ces autorités et leurs responsabilités connexes peuvent être associées ou intégrées dans la même entité structurée ou se partager entre différentes entités structurées, à condition que l'on veille à éviter au niveau interne tout conflit d'intérêt et tout chevauchement des tâches.

Autorité chargée de l'assurance de l'information (AAI)

43. L'AAI s'acquitte des tâches suivantes:

a) définir les lignes directrices de sécurité en matière d'AI et en surveiller l'efficacité et la pertinence;

b) conserver et gérer les données techniques relatives aux produits cryptographiques;

c) veiller à ce que les mesures en matière d'AI sélectionnées aux fins de la protection des ICUE soient conformes aux lignes directrices régissant leur éligibilité et leur sélection;

d) veiller à ce que les produits cryptographiques soient sélectionnés conformément aux lignes directrices régissant leur éligibilité et leur sélection;

e) coordonner la formation et la sensibilisation à l'AI;

f) mener des consultations avec le fournisseur du système, les intervenants en matière de sécurité et les représentants des utilisateurs au sujet des lignes directrices de sécurité en matière d'AI; et

g) veiller à ce que les sous-divisions spécialisées du comité de sécurité du SEAE disposent des compétences requises en matière d'AI.

Autorité TEMPEST

44. L'autorité TEMPEST (AT) est chargée de veiller à la conformité des SIC aux stratégies et lignes directrices TEMPEST. Elle approuve les contre-mesures TEMPEST pour les installations et les produits destinés à protéger des ICUE jusqu'à un certain niveau de classification dans leur environnement opérationnel.

Autorité d'agrément cryptographique (AAC)

45. L'AAC est chargée de veiller à ce que les produits cryptographiques soient conformes aux lignes directrices respectives en matière cryptographique. Elle agrée les produits cryptographiques pour la protection d'ICUE jusqu'à un certain niveau de classification dans leur environnement opérationnel.

Autorité chargée de la distribution cryptographique (ADC)

46. L'ADC est chargé des tâches suivantes:

a) gérer le matériel cryptographique de l'UE et en rendre compte;

b) veiller à ce que les procédures et les circuits appropriés soient mis en place pour rendre compte de tout le matériel cryptographique de l'UE et en assurer la manutention, le stockage et la distribution en toute sécurité; et

c) assurer le transfert et la reprise du matériel cryptographique de l'UE auprès des personnes ou des services utilisateurs.

Autorité d'homologation de sécurité (AHS)

47. L'autorité d'homologation de sécurité de chaque système s'acquitte des tâches suivantes:

a) veiller à ce que les SIC soient conformes aux lignes directrices de sécurité pertinentes, délivrer une déclaration d'homologation pour les SIC en vue du traitement des ICUE jusqu'à un certain niveau de classification dans leur environnement opérationnel et indiquant les conditions et modalités de l'homologation ainsi que les critères dont l'existence justifie une nouvelle homologation;

b) mettre en place un processus d'homologation de sécurité conforme aux lignes directrices pertinentes et indiquant clairement les conditions d'homologation que doivent remplir les SIC relevant de sa responsabilité;

c) définir une stratégie d'homologation de sécurité qui indique le niveau de précision du processus d'homologation en fonction du niveau d'assurance requis;

d) étudier et approuver les documents se rapportant à la sécurité, y compris en ce qui concerne la gestion des risques et les énoncés des risques résiduels, les énoncés des impératifs de sécurité propres à un système (ci-après «SSRS»), les documents concernant la vérification de la mise en œuvre des mesures de sécurité et les procédures d'exploitation de sécurité (ci-après «SecOP»), et veiller à ce qu'ils soient conformes aux lignes directrices et aux règles du SEAE en matière de sécurité;

e) vérifier la mise en œuvre des mesures de sécurité en rapport avec les SIC en effectuant elle-même ou en finançant des évaluations, des inspections ou des réexamens en la matière;

f) définir les exigences en matière de sécurité (par exemple les niveaux d'habilitation de sécurité du personnel) applicables aux postes sensibles dans le cadre d'un SIC;

g) accepter la sélection des produits cryptographiques et TEMPEST ayant fait l'objet d'une approbation qui sont utilisés pour assurer la sécurité d'un SIC;

h) approuver, le cas échéant dans le cadre d'une approbation conjointe, l'interconnexion d'un SIC à d'autres SIC; et

i) mener des consultations avec le fournisseur du système, les intervenants en matière de sécurité et les représentants des utilisateurs au sujet de la gestion des risques de sécurité, et notamment du risque résiduel, et des conditions et modalités de la déclaration d'homologation.

48. L'AHS du SEAE est chargée de l'homologation de tous les SIC exploités dans le cadre de la compétence du SEAE.

Comité d'homologation de sécurité (CHS)

49. Un comité conjoint d'homologation de sécurité (CHS) est chargé de l'homologation des SIC qui sont du ressort aussi bien de l'AHS du SEAE que des AHS des États membres. Ce comité est composé d'un représentant de l'AHS de chaque État membre, un représentant de l'AHS du SCG et de la Commission assistant à ses réunions. Les autres entités disposant de nœuds de connexion avec un SIC sont invitées à assister aux réunions lorsque celles-ci portent sur le système considéré.

Le CHS est présidé par un représentant de l'AHS du SEAE. Il statue par consensus entre les représentants des AHS des institutions, des États membres et des autres entités disposant de nœuds de connexion avec le SIC considéré. Le CHS rend compte à intervalles réguliers de ses activités au comité de sécurité du SEAE et notifie à celui-ci toute déclaration d'homologation.

Autorité opérationnelle chargée de l'assurance de l'information

50. L'autorité opérationnelle chargée de l'AI pour chaque système s'acquitte des tâches suivantes:

a) élaborer des documents relatifs à la sécurité conformes aux lignes directrices en matière de sécurité, notamment l'énoncé des impératifs de sécurité propres à un système («**SSRS**»), y compris en ce qui concerne le risque résiduel, les procédures d'exploitation de sécurité («**SecOP**») et le volet cryptographique du processus d'homologation des SIC;

b) participer à la sélection et à la mise à l'essai des mesures, dispositifs et logiciels de sécurité technique propres à un système, superviser leur mise en œuvre et s'assurer qu'ils sont installés, configurés et entretenus de manière sûre conformément aux documents de sécurité pertinents;

c) participer à la sélection des mesures et des dispositifs de sécurité TEMPEST lorsque les SSRS le prévoient, et veiller à ce qu'ils soient installés et entretenus de manière sûre en coopération avec l'AT;

d) assurer le suivi de la mise en œuvre et de l'application des SecOP et, s'il y a lieu, déléguer les responsabilités opérationnelles de sécurité au détenteur du système;

e) gérer et utiliser les produits cryptographiques, assurer la protection des éléments chiffrés et contrôlés et, au besoin, assurer la production de variables cryptographiques;

f) procéder au réexamen et à des analyses de sécurité et à des tests, notamment afin d'établir les rapports nécessaires sur les risques encourus, comme l'exige l'AHS;

g) dispenser une formation sur l'AI propre à chaque SIC;

h) mettre en œuvre et gérer des mesures de sécurité propres à chaque SIC.

ANNEXE A V

SÉCURITÉ INDUSTRIELLE

I. INTRODUCTION

1. La présente annexe contient les modalités d'application de l'article 9 de l'annexe A. Elle prévoit des dispositions de sécurité générales applicables aux entités industrielles ou autres dans le cadre de négociations précontractuelles et tout au long du cycle de vie de contrats classifiés attribués par le SEAE.

2. L'autorité de sécurité du SEAE approuve des lignes directrices de sécurité industrielle indiquant en particulier les modalités précises en ce qui concerne les habilitations de sécurité d'établissement («HSE»), les annexes de sécurité («AS»), les visites, la transmission et le transport d'ICUE.

II. ASPECTS LIÉS À LA SÉCURITÉ DANS UN CONTRAT CLASSIFIÉ

Guide de la classification de sécurité (GCS)

3. Avant de lancer un appel d'offres en vue de l'attribution d'un contrat classifié ou d'attribuer un tel contrat, le SEAE, en sa qualité d'autorité contractante, détermine la classification de sécurité de toute information devant être fournie aux soumissionnaires et aux contractants, ainsi que la classification de sécurité de toute information devant être créée par le contractant. Dans cette perspective, le SEAE élabore un guide de la classification de sécurité (GCS), qui sera utilisé aux fins de l'exécution du contrat.

4. Les principes ci-après sont appliqués pour déterminer le niveau de classification de sécurité des différents éléments d'un contrat classifié:

   a) dans le cadre de l'élaboration d'un GCS, le SEAE tient compte de tous les aspects pertinents en matière de sécurité, y compris de la classification de sécurité attribuée aux informations fournies et dont l'utilisation aux fins du contrat a été approuvée par l'autorité d'origine desdites informations;

   b) le niveau général de classification du contrat ne peut pas être inférieur à la classification la plus élevée de l'un de ses éléments; et

   c) le cas échéant, le SEAE se met en rapport avec les ANS/ASD ou toute autre autorité de sécurité compétente des États membres dans l'éventualité d'une modification touchant au niveau de classification des informations créées par les contractants ou fournies à ceux-ci dans le cadre de l'exécution d'un contrat et lors de toute modification ultérieure du GCS.

Annexe de sécurité (AS)

5. Les impératifs de sécurité propres à un contrat sont exposés dans une AS. Le cas échéant, l'AS contient le GCS et fait partie intégrante du contrat ou du contrat de sous-traitance classifié.

6. L'AS contient les dispositions imposant au contractant et/ou au sous-traitant de respecter les normes minimales énoncées dans la présente décision. Le non-respect de ces normes minimales peut constituer un motif suffisant de résiliation du contrat.

Instructions de sécurité relatives à un programme/un projet (ISP)

7. En fonction de la portée des programmes ou des projets impliquant l'accès à des ICUE ou leur traitement ou stockage, l'autorité contractante chargée de gérer le projet ou le programme considéré peut élaborer des instructions de sécurité relatives à un programme/un projet (ISP). Les ISP doivent être approuvées par les ANS/ASD ou toute autre autorité de sécurité compétente des États membres associées au programme/projet et peuvent contenir d'autres exigences en matière de sécurité.

III. HABILITATION DE SÉCURITÉ D'ÉTABLISSEMENT (HSE)

8. La direction du SEAE chargée de la sécurité demande à l'ANS/ASD ou toute autre autorité de sécurité compétente d'un État membre de délivrer une HSE afin d'indiquer, conformément aux dispositions législatives et réglementaires nationales, que l'entité industrielle ou autre est en mesure, au sein de ses établissements, de garantir aux ICUE la protection adaptée au niveau de classification approprié (CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET). L'accès aux ICUE n'est ni fourni ni accordé à un contractant ou sous-traitant, réel ou potentiel, tant qu'il n'a pas prouvé auprès du SEAE qu'il dispose d'une HSE.

9. S'il y a lieu, le SEAE, en sa qualité d'autorité contractante, avertit l'ANS/ASD ou toute autre autorité de sécurité compétente qu'une HSE est nécessaire dans la phase précontractuelle ou pour l'exécution du contrat. Une HSE ou une HSP est requise dans la phase précontractuelle lorsque des ICUE CONFIDENTIEL UE/EU CONFIDENTAL ou SECRET UE/EU SECRET doivent être fournies dans la phase de soumission des offres.

10. Le SEAE, en sa qualité d'autorité contractante, n'attribue pas de contrat classifié au soumissionnaire sélectionné tant que l'ANS/ASD ou toute autre autorité de sécurité compétente de l'État membre dans lequel le contractant ou le sous-traitant concerné est immatriculé ne lui a pas confirmé qu'une HSE appropriée a été délivrée.

11. Le SEAE, en sa qualité d'autorité contractante, demande à l'ANS/ASD ou toute autre autorité de sécurité compétente ayant délivré une HSE de lui notifier toute information défavorable affectant ladite HSE. Dans le cadre d'un contrat de sous-traitance, l'ANS/ASD ou toute autre autorité de sécurité compétente en est informée.

12. Le retrait d'une HSE par l'ANS/ASD concernée ou toute autre autorité de sécurité compétente constitue pour le SEAE, en sa qualité d'autorité contractante, un motif suffisant pour résilier un contrat classifié ou exclure un soumissionnaire de la procédure d'appel d'offres.

IV. HABILITATIONS DE SÉCURITÉ DU PERSONNEL (HSP) POUR LE PERSONNEL DES CONTRACTANTS

13. Toutes les personnes travaillant pour des contractants ayant besoin d'un accès à des ICUE classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur doivent avoir reçu une habilitation de sécurité adéquate et avoir un besoin d'en connaître pour pouvoir accéder aux informations. Bien qu'une HSP ne soit pas nécessaire pour pouvoir accéder aux ICUE RESTREINT UE/EU RESTRICTED, les personnes concernées devront faire état d'un besoin d'en connaître pour y accéder.

14. Les demandes d'HSP pour les membres du personnel de contractants sont adressées à l'ANS/ASD responsable de l'entité concernée.

15. Le SEAE attire l'attention des contractants souhaitant employer un ressortissant d'un État tiers à un poste nécessitant un accès aux ICUE sur le fait qu'il est de la responsabilité de l'ANS/ASD de l'État membre dans lequel est située et constituée l'entité qui recrute de déterminer si la personne concernée peut accéder à de telles informations, conformément à la présente décision, et de confirmer que l'autorité d'origine doit avoir donné son consentement avant l'octroi de l'accès en question.

V. CONTRATS ET CONTRATS DE SOUS-TRAITANCE CLASSIFIÉS

16. Lorsque des ICUE sont communiquées à un soumissionnaire durant la phase précontractuelle, l'appel d'offres contient une disposition prévoyant que le soumissionnaire qui ne présente pas d'offre ou qui n'est pas sélectionné sera tenu de restituer tous les documents classifiés dans un délai spécifié.

17. Une fois qu'un contrat ou un contrat de sous-traitance classifié a été attribué, le SEAE, en sa qualité d'autorité contractante, notifie les dispositions en matière de sécurité que comporte le contrat classifié à l'ANS/ASD ou à toute autre autorité de sécurité compétente dont relève le contractant ou le sous-traitant.

18. À l'expiration ou à la résiliation d'un tel contrat, le SEAE, en sa qualité d'autorité contractante, (et/ou l'ANS/ASD ou toute autre autorité de sécurité compétente, selon qu'il conviendra, dans le cas d'un contrat de sous-traitance) avertit immédiatement l'ANS/ASD ou toute autre autorité de sécurité compétente de l'État membre dans lequel le contractant ou le sous-traitant est immatriculé.

19. En principe, le contractant ou le sous-traitant est tenu de restituer à l'autorité contractante les ICUE en sa possession, dès que le contrat ou le contrat de sous-traitance classifié arrive à expiration ou est résilié.

20. Des dispositions spéciales concernant l'élimination d'ICUE durant l'exécution du contrat ou à son expiration ou à sa résiliation figurent dans l'AS.

21. Lorsque le contractant ou le sous-traitant est autorisé à conserver des ICUE après l'expiration ou la résiliation d'un contrat, les normes minimales figurant dans la présente demeurent d'application et la confidentialité des ICUE est protégée par le contractant ou le sous-traitant.

22. Les conditions dans lesquelles le contractant peut sous-traiter des activités sont définies dans l'invitation à soumissionner et le contrat.

23. Un contractant doit obtenir l'autorisation du SEAE, en sa qualité d'autorité contractante, avant de pouvoir sous-traiter des éléments d'un contrat classifié. Aucun contrat de sous-traitance ne peut être attribué à des entités industrielles ou autres immatriculées dans un État non membre de l'Union européenne n'ayant pas conclu avec l'UE un accord sur la sécurité des informations.

24. Il incombe au contractant de veiller à ce que toutes les activités de sous-traitance soient réalisées en conformité avec les normes minimales définies dans la présente décision et de s'abstenir de fournir des ICUE à un sous-traitant sans l'autorisation écrite préalable de l'autorité contractante.

25. En ce qui concerne les ICUE créées ou traitées par le contractant ou le sous-traitant, les droits qui incombent à l'autorité d'origine sont exercés par l'autorité contractante.

VI. VISITES LIÉES À DES CONTRATS CLASSIFIÉS

26. Lorsque le SEAE, les contractants ou les sous-traitants doivent avoir accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET dans leurs locaux respectifs aux fins de l'exécution d'un contrat classifié, les visites sont organisées en liaison avec les ANS/ASD ou toute autre autorité de sécurité compétente concernée. Et ce sans préjudice du pouvoir des ANS/ASD, dans le cadre de projets spécifiques, de convenir d'une procédure permettant d'organiser directement de telles visites.

27. Tous les visiteurs sont en possession d'une HSP adéquate et jouissent d'un accès aux ICUE liées au contrat attribué par le SEAE sur la base du principe du besoin d'en connaître.

28. Les visiteurs se voient uniquement accorder l'accès aux ICUE liées à l'objectif de la visite.

VII. TRANSMISSION ET TRANSPORT DES ICUE

29. En ce qui concerne la transmission des ICUE par voie électronique, les dispositions pertinentes de l'article 8 et de l'annexe A IV s'appliquent.

30. En ce qui concerne le transport d'ICUE, les dispositions pertinentes de l'annexe A III s'appliquent, conformément aux dispositions législatives et réglementaires nationales.

31. En ce qui concerne le transport de matériel classifié en tant que fret, les principes ci-après s'appliquent pour déterminer les mesures de sécurité à mettre en œuvre:

    a) la sécurité est assurée à tous les stades pendant le transport, du point d'origine jusqu'à la destination finale;

    b) le degré de protection accordé à un envoi est déterminé en fonction du niveau de classification le plus élevé du matériel qu'il contient;

    c) une HSE du niveau approprié est obtenue pour les sociétés assurant le transport, s'il implique également le stockage des informations classifiées dans les installations des contractants. Quoi qu'il en soit, le personnel manipulant l'envoi fait l'objet d'une habilitation de sécurité appropriée conformément à l'annexe A I;

d) avant tout transfert transfrontalier de matériel classifié CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, un plan de transport est établi par l'expéditeur et approuvé par le SEAE, le cas échéant en liaison avec les ANS/ASD tant de l'expéditeur que du destinataire ou toute autre autorité de sécurité compétente concernée;

e) les trajets sont directs dans la mesure du possible, et aussi rapides que les circonstances le permettent;

f) chaque fois que cela est possible, les itinéraires ne devraient passer que par des États membres. Les itinéraires passant par des États autres que les États membres ne devraient être suivis qu'à condition d'avoir été autorisés par le SEAE ou toute autre autorité de sécurité compétente des États de l'expéditeur et du destinataire.

VIII. TRANSFERT D'ICUE AUX CONTRACTANTS ÉTABLIS DANS DES PAYS TIERS

32. Les ICUE sont transférées aux contractants et sous-traitants établis dans des pays tiers ayant conclu un accord de sécurité valide avec l'UE conformément aux mesures de sécurité convenues entre le SEAE, en sa qualité d'autorité contractante, et l'ANS/ASD du pays tiers concerné dans lequel le contractant est immatriculé.

IX. TRAITEMENT ET CONSERVATION D'INFORMATIONS CLASSIFIÉES RESTREINT UE/EU RESTRICTED

33. En liaison, s'il y a lieu, avec l'ANS/ASD de l'État membre, le SEAE, en sa qualité d'autorité contractante, est habilité à effectuer des visites dans les établissements des contractants/sous-traitants, en vertu de dispositions contractuelles, afin de vérifier que les mesures de sécurité adaptées pour la protection des ICUE de niveau RESTREINT UE/EU RESTRICTED ont été mises en place, comme l'exige le contrat.

34. Dans la mesure où cela est nécessaire en vertu des dispositions législatives et réglementaires nationales, les ANS/ASD, ou toute autre autorité de sécurité compétente, doivent être informées par le SEAE, en sa qualité d'autorité contractante, des contrats ou des contrats de sous-traitance contenant des informations classifiées RESTREINT UE/EU RESTRICTED.

35. Les contractants ou sous-traitants et leur personnel ne sont pas tenus d'être en possession d'une HSE ou d'une HSP pour les contrats attribués par le SEAE qui comportent des informations classifiées RESTREINT UE/EU RESTRICTED.

36. Le SEAE, en sa qualité d'autorité contractante, examine les réponses aux appels d'offres portant sur des contrats nécessitant l'accès à des informations classifiées RESTREINT UE/EU RESTRICTED, nonobstant les exigences en matière d'HSE ou d'HSP pouvant être prévues par les dispositions législatives et réglementaires nationales.

37. Les conditions régissant la sous-traitance d'activités par un contractant sont conformes aux paragraphes 22, 23 et 24.

38. Lorsqu'un contrat prévoit le traitement d'informations classifiées RESTREINT UE/EU RESTRICTED dans un SIC exploité par un contractant, le SEAE, en sa qualité d'autorité contractante, veille à ce que les exigences techniques et administratives à remplir concernant l'homologation du SIC soient précisées dans le contrat ou tout contrat de sous-traitance; ces exigences sont proportionnées au risque évalué, compte tenu de tous les facteurs pertinents. La portée de l'homologation dudit SIC est décidée d'un commun accord par l'autorité contractante et l'ANS/ASD compétente.

ANNEXE A VI

ÉCHANGE D'INFORMATIONS CLASSIFIÉES AVEC DES PAYS TIERS ET DES ORGANISATIONS INTERNATIONALES

I. INTRODUCTION

1. La présente annexe énonce les modalités d'application de l'article 10 de l'annexe A.

II. CADRES RÉGISSANT L'ÉCHANGE D'INFORMATIONS CLASSIFIÉES

2. Le SEAE peut échanger des ICUE avec des pays tiers ou des organisations internationales conformément à l'article 10, paragraphe 1, de l'annexe A.

Afin d'aider la HR dans les responsabilités qui lui incombent en vertu de l'article 218 du TFUE:

a) le département géographique ou thématique concerné du SEAE relève, en concertation avec la direction du SEAE chargée de la sécurité, la nécessité de procéder à un échange à long terme d'ICUE avec l'organisation internationale ou le pays tiers concerné, le cas échéant;

b) la direction du SEAE chargée de la sécurité soumet à la HR, après avoir consulté le département géographique concerné du SEAE, les projets de textes à proposer au Conseil, en vertu de l'article 218, paragraphes 3, 5 et 6, du TFUE, le cas échéant;

c) la direction du SEAE chargée de la sécurité soutient la HR dans la conduite de négociations, en coordination avec les services concernés de la Commission et du Secrétariat général du Conseil;

d) pour ce qui est des accords ou des arrangements conclus avec des pays tiers au sujet de leur participation à des opérations PESD de gestion de crise visés à l'article 10, paragraphe 1, point c), de l'annexe A, la direction «Gestion des crises et planification» du SEAE soumet à la HR, après avoir consulté les services concernés du SEAE, les projets de textes à proposer au Conseil en vertu de l'article 218, paragraphes 3, 5 et 6, du TFUE et soutient la HR dans la conduite des négociations en coordination avec les services concernés du SEAE et du Secrétariat général du Conseil, le cas échéant.

3. Dans les cas où les accords sur la sécurité des informations prévoient des modalités techniques d'application à convenir entre la direction du SEAE chargée de la sécurité — en coordination avec la direction de la sécurité de la direction générale des ressources humaines et de la sécurité de la Commission et le bureau de sécurité du Secrétariat général du Conseil — et l'autorité de sécurité compétente de l'État tiers ou de l'organisation internationale en question, de tels arrangements tiennent compte du niveau de protection prévu par les règlements, les structures et les procédures de sécurité en place dans le pays tiers ou l'organisation internationale concerné.

4. Lorsqu'il existe un besoin durable pour le SEAE d'échanger, avec un pays tiers ou une organisation internationale, des informations dont le niveau de classification n'est en principe pas supérieur à RESTREINT UE/EU RESTRICTED, et qu'il a été établi que la partie en question ne dispose pas d'un système de sécurité suffisamment développé lui permettant de conclure un accord sur la sécurité des informations, la HR peut, sous réserve de l'avis unanimement favorable de la direction de la sécurité du SEAE conformément à l'article 15, paragraphe 5, de la présente décision, conclure un arrangement administratif avec les autorités compétentes du pays tiers ou de l'organisation internationale concerné(e).

5. Les ICUE ne font l'objet d'aucun échange par voie électronique avec un pays tiers ou une organisation internationale, sauf disposition expresse de l'accord sur la sécurité des informations ou de l'arrangement administratif.

6. Conformément à un éventuel arrangement administratif sur l'échange d'informations classifiées, le SEAE et le pays tiers ou l'organisation internationale désignent chacun un bureau d'ordre qui fera office de principal point d'entrée et de sortie pour les informations classifiées échangées. Pour le SEAE, il s'agit de son bureau d'ordre central.

7. Les arrangements administratifs prennent, en règle générale, la forme d'un échange de lettres.

III. VISITES D'ÉVALUATION

8. Les visites d'évaluation visées à l'article 17 de la présente décision sont réalisées d'un commun accord avec le pays tiers ou l'organisation internationale concerné(e), et sont axées sur:

   a) le cadre réglementaire applicable à la protection des informations classifiées;

   b) toute caractéristique spécifique des dispositions législatives et réglementaires, politiques ou procédures en matière de sécurité du pays tiers ou de l'organisation internationale susceptibles d'avoir une incidence sur le niveau maximal de classification des ICUE qui peuvent être échangées;

   c) les mesures et procédures de sécurité en vigueur pour la protection des informations classifiées; et

   d) les procédures d'habilitation de sécurité pour le niveau de classification des ICUE à communiquer.

9. Les ICUE ne font l'objet d'aucun échange avant qu'une visite d'évaluation n'ait été conduite et que le niveau auquel les informations classifiées peuvent être échangées entre les parties n'ait été déterminé, sur la base de l'équivalence du niveau de protection qui leur sera attribué.

   Si, dans l'attente d'une telle visite d'évaluation, une raison exceptionnelle ou urgente d'échanger des informations classifiées est portée à la connaissance de la HR, le SEAE:

   a) demande tout d'abord le consentement écrit de l'autorité d'origine afin d'établir l'absence d'objection à la communication;

   b) s'en réfère à l'autorité de sécurité du SEAE, qui peut décider de communiquer les informations concernées, après obtention de l'avis unanimement favorable des États membres tels que représentés au comité de sécurité du SEAE.

   Si, toutefois, le SEAE est dans l'impossibilité de déterminer l'autorité d'origine, l'autorité de sécurité du SEAE endosse la responsabilité de l'autorité d'origine après avoir obtenu l'avis unanimement favorable du comité de sécurité du SEAE.

IV. AUTORISATION DE COMMUNIQUER DES ICUE À DES PAYS TIERS OU À DES ORGANISATIONS INTERNATIONALES

10. En présence d'un accord d'échange d'informations classifiées avec un pays tiers ou une organisation internationale en vertu de l'article 10, paragraphe 1, de l'annexe A, la décision de communiquer des ICUE par le SEAE à un pays tiers ou une organisation internationale est prise par l'autorité de sécurité du SEAE, qui peut déléguer cette autorisation à de hauts fonctionnaires du SEAE ou à d'autres personnes sous son autorité.

11. Si l'autorité d'origine des informations classifiées à communiquer, y compris les autorités d'origine des sources qu'elles peuvent contenir, n'est pas le SEAE, ce dernier demande tout d'abord à l'autorité d'origine de confirmer par écrit qu'elle ne s'oppose pas à la communication des informations en question. Si le SEAE est dans l'impossibilité de déterminer l'autorité d'origine, l'autorité de sécurité du SEAE endosse la responsabilité de l'autorité d'origine après avoir obtenu l'avis unanimement favorable des États membres représentés au sein du comité de sécurité du SEAE.

V. COMMUNICATION AD HOC EXCEPTIONNELLE D'ICUE

12. En l'absence de l'un des cadres visés à l'article 10, paragraphe 1, de l'annexe A, et dans les cas où les intérêts de l'UE ou d'un ou de plusieurs États membres requièrent la communication d'ICUE pour des raisons politiques, opérationnelles ou urgentes, les ICUE peuvent exceptionnellement être communiquées à un pays tiers ou une organisation internationale dès que les mesures suivantes ont été prises.

   Après s'être assurée que les conditions énumérées au paragraphe 11 ci-dessus sont réunies, la direction du SEAE chargée de la sécurité:

   a) vérifie, dans la mesure du possible, auprès des autorités de sécurité du pays tiers ou de l'organisation internationale concerné(e) que son règlement, ses structures et ses procédures de sécurité permettent de garantir que les ICUE qui lui seront communiquées bénéficieront d'une protection conforme à des normes qui ne sont pas moins strictes que celles prévues dans la présente décision;

b) invite le comité de sécurité du SEAE à formuler, sur la base des informations disponibles, un avis concernant la confiance qui peut être accordée au règlement, aux structures et aux procédures de sécurité en vigueur dans le pays tiers ou l'organisation internationale auquel les ICUE doivent être communiquées;

c) s'en réfère à l'autorité de sécurité du SEAE, qui peut décider de communiquer les informations concernées, après obtention de l'avis unanimement favorable des États membres tels que représentés au comité de sécurité du SEAE.

13. En l'absence de l'un des cadres visés à l'article 10, paragraphe 1, de l'annexe A, la tierce partie en question s'engage par écrit à protéger adéquatement les ICUE.

Appendice A

Définitions

Aux fins de la présente décision, on entend par:

«homologation»: la procédure conduisant à une déclaration formelle de l'autorité d'homologation de sécurité (AHS) indiquant qu'un système est agréé pour fonctionner à un niveau de classification déterminé, selon un mode d'exploitation de sécurité spécifique dans son environnement opérationnel et à un niveau de risque acceptable, pour autant qu'un ensemble approuvé de mesures de sécurité ait été mis en place sur le plan technique et physique, ainsi qu'au niveau de l'organisation et des procédures;

«ressource»: tout ce qui présente de l'utilité pour une organisation, ses activités et la continuité de celles-ci, y compris les ressources en matière d'information dont l'organisation a besoin pour s'acquitter de sa mission;

«autorisation d'accès aux ICUE»: une autorisation que prend l'autorité de sécurité du SEAE en conformité avec la présente décision après qu'une HSP a été délivrée par les autorités compétentes d'un État membre, attestant qu'une personne peut, pour autant que son besoin d'en connaître ait été établi, être autorisée à avoir accès aux ICUE jusqu'à un niveau de classification donné (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur) jusqu'à une date donnée — voir article 2 de l'annexe A I;

«infraction»: un acte ou une omission commis par une personne qui est contraire aux règles de sécurité énoncées dans la présente décision et/ou aux politiques ou lignes directrices en matière de sécurité énonçant les éventuelles mesures nécessaires à sa mise en œuvre;

«cycle de vie d'un SIC»: la durée totale d'existence d'un SIC, laquelle comprend le lancement, la conception, la planification, l'analyse des besoins, l'élaboration, le développement, la mise à l'essai, la mise en œuvre, l'exploitation, la maintenance et le démantèlement;

«contrat classifié»: un contrat conclu par le SEAE avec un contractant en vue de la fourniture de biens, de la réalisation de travaux ou de la prestation de services, dont l'exécution requiert ou implique l'accès à des ICUE ou la création de telles informations;

«contrat de sous-traitance classifié»: un contrat conclu par un contractant du SEAE avec un autre contractant (c'est-à-dire le sous-traitant) en vue de la fourniture de biens, de la réalisation de travaux ou de la prestation de services, dont l'exécution nécessite ou implique l'accès à des informations classifiées de l'Union européenne ou la production de telles informations;

«système d'information et de communication» (SIC): tout système permettant le traitement d'informations sous forme électronique. Un système d'information et de communication comprend l'ensemble des moyens nécessaires pour le faire fonctionner, y compris l'infrastructure, l'organisation, le personnel et les ressources d'information — voir article 8, paragraphe 2, de l'annexe A;

«compromission d'ICUE»: la divulgation totale ou partielle d'ICUE à des personnes ou entités non autorisées — voir article 9, paragraphe 2;

«contractant»: une personne ou une entité juridique dotées de la capacité juridique de conclure des contrats;

«produits cryptographiques»: les algorithmes cryptographiques, les modules matériels et logiciels cryptographiques, et les produits comprenant les modalités de mise en œuvre et la documentation y relative, ainsi que les éléments de mise à la clé;

«opération PSDC»: une opération militaire ou civile de gestion de crise mise en place en vertu du titre V, chapitre 2, du TUE;

«déclassification»: la suppression de toute classification de sécurité;

«défense en profondeur»: l'application d'un éventail de mesures de sécurité organisées en plusieurs niveaux de défense;

«autorité de sécurité désignée» (ASD): l'autorité responsable devant l'autorité nationale de sécurité (ANS) d'un État membre qui est chargée de communiquer à des entités industrielles ou autres la politique nationale dans tous les domaines relevant de la sécurité industrielle et de fournir des orientations et une aide pour sa mise en œuvre. Les fonctions de l'ASD peuvent être exercées par l'ANS ou par toute autre autorité compétente;

«document»: toute information enregistrée quelles que soient sa forme ou ses caractéristiques physiques;

«déclassement»: le passage à un niveau de classification de sécurité inférieur;

«informations classifiées de l'UE» (ICUE): toute information ou tout matériel identifié comme tel par une classification de sécurité de l'UE, dont la divulgation non autorisée pourrait porter atteinte à des degrés divers aux intérêts de l'Union européenne, ou à ceux d'un ou de plusieurs de ses États membres — voir article 2, point f);

«habilitation de sécurité d'établissement (HSE)»: une décision administrative prise par une ANS ou une ASD selon laquelle, du point de vue de la sécurité, un établissement peut assurer un niveau suffisant de protection pour les ICUE d'un niveau de classification de sécurité déterminé et selon laquelle le personnel de l'établissement qui doit accéder à des ICUE possède une habilitation de sécurité appropriée et a été informé des conditions de sécurité requises pour accéder à des ICUE et les protéger;

«traitement» d'ICUE: l'ensemble des actions dont les ICUE sont susceptibles de faire l'objet tout au long de leur cycle de vie; sont ainsi visés leur création, leur traitement, leur transport, leur déclassement, leur déclassification et leur destruction. En ce qui concerne les SIC, sont en outre compris leur collecte, leur affichage, leur transmission et leur stockage;

«détenteur»: une personne dûment autorisée qui, sur la base d'un besoin d'en connaître avéré, est en possession d'un élément d'ICUE et à laquelle il incombe par conséquent d'en assurer la protection;

«entité industrielle ou autre»: une entité s'occupant de la fourniture de biens, de la réalisation de travaux ou de la prestation de services; il peut s'agir d'une entité industrielle, commerciale ou scientifique, ou d'une entité de service, de recherche, d'enseignement ou de développement ou d'une personne exerçant une activité indépendante;

«sécurité industrielle»: l'application de mesures visant à assurer la protection des ICUE par des contractants ou des sous-traitants dans le cadre de négociations précontractuelles et tout au long du cycle de vie des contrats classifiés — voir article 9, paragraphe 1, de l'annexe A;

«assurance de l'information» (AI) dans le domaine des systèmes d'information et de communication: la certitude que ces systèmes protégeront les informations qu'ils traitent et fonctionneront comme ils le doivent, quand ils le doivent, sous le contrôle d'utilisateurs légitimes. Une AI efficace garantit des niveaux appropriés de confidentialité, d'intégrité, de disponibilité, de non-répudiation et d'authenticité. L'AI est fondée sur un processus de gestion des risques — voir article 8, paragraphe 1, de l'annexe A;

«interconnexion»: aux fins de la présente décision, la connexion directe d'au moins deux systèmes informatiques permettant à ceux-ci d'échanger des données et d'autres ressources en matière d'information (communication, par exemple) de façon unidirectionnelle ou multidirectionnelle — voir annexe A IV, paragraphe 31;

«gestion des informations classifiées»: l'application de mesures administratives pour contrôler les ICUE tout au long de leur cycle de vie afin de compléter les mesures prévues aux articles 5, 6 et 8 et de contribuer ainsi à la dissuasion, à la détection et au retour aux conditions opérationnelles dans le cadre de la compromission ou de la perte délibérée ou accidentelle de telles informations. Ces mesures concernent en particulier la création, l'enregistrement, la duplication, la traduction, le transport, le traitement, le stockage et la destruction des ICUE — voir article 7, paragraphe 1, de l'annexe A;

«matériel»: tout document ou élément de machine ou d'équipement, déjà fabriqué ou en cours de fabrication;

«autorité d'origine»: l'institution, l'organe ou l'organisme de l'UE, l'État membre, le pays tiers ou l'organisation internationale sous l'autorité de laquelle les informations classifiées ont été créées et/ou introduites dans les structures de l'UE;

«mesures de sécurité concernant le personnel»: l'application de mesures visant à faire en sorte que l'accès aux ICUE ne soit accordé qu'aux personnes qui ont:

— un besoin d'en connaître,

— en ce qui concerne l'accès à des informations CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, ont fait l'objet d'une habilitation de sécurité du niveau correspondant, ou ont été dûment autorisées en vertu de leurs fonctions conformément aux lois et réglementations nationales, et

— été informées de leurs responsabilités —

voir article 5, paragraphe 1, de l'annexe A;

«habilitation de sécurité du personnel» (HSP) donnant accès aux ICUE: une autorisation émanant de l'autorité investie du pouvoir de nomination du SGC conformément à la présente décision à la suite d'une enquête de sécurité menée par les autorités compétentes d'un État membre et attestant qu'une personne peut, pour autant que son besoin d'en connaître ait été établi, être autorisée à avoir accès aux ICUE jusqu'à un niveau de classification donné (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur) jusqu'à une date donnée; la personne ainsi décrite est «habilitée»;

«certificat d'habilitation de sécurité du personnel (CHSP)»: un certificat délivré par une autorité compétente attestant qu'une personne a obtenu une habilitation de sécurité et détient une HSP ou une autorisation valable accordée par le chef de la direction chargée de la sécurité et permettant l'accès à des ICUE, et indiquant le niveau de classification des ICUE auxquelles la personne peut être autorisée à avoir accès (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur), la durée de validité de l'HSP correspondante et la date d'expiration du certificat;

«sécurité physique»: l'application de mesures physiques et techniques de protection pour dissuader l'accès non autorisé aux ICUE — voir article 6 de l'annexe A;

«instructions de sécurité relatives à un programme/un projet» (ISP): une liste des procédures de sécurité appliquées à un programme ou à un projet spécifique en vue d'uniformiser ces procédures. Elles peuvent être revues tout au long de la durée du programme ou du projet;

«enregistrement»: l'application de procédures permettant de garder la trace du cycle de vie d'une information, y compris de sa diffusion et de sa destruction voir annexe A III, paragraphe 21;

«risque résiduel»: le risque qui subsiste après que des mesures de sécurité ont été mises en œuvre, étant entendu qu'il est impossible de contrer toutes les menaces et d'éliminer toutes les vulnérabilités;

«risque»: la possibilité qu'une menace donnée se concrétise en tirant parti des vulnérabilités internes et externes d'une organisation ou d'un des systèmes qu'elle utilise et cause ainsi un préjudice à l'organisation ou à ses ressources matérielles ou immatérielles. Il se mesure en tenant compte à la fois de la probabilité de voir se concrétiser des menaces et de l'incidence de celles-ci;

«acceptation des risques»: la décision d'accepter qu'un risque résiduel subsiste au terme du traitement des risques;

«évaluation des risques»: le fait de déterminer les menaces et les vulnérabilités et à procéder à l'analyse des risques correspondants, c'est-à-dire à examiner leur probabilité et leur incidence;

«communication des risques»: le fait de sensibiliser la communauté des utilisateurs du SIC aux risques, d'informer les autorités d'homologation de ces risques et de faire rapport à leur sujet aux autorités responsables de l'exploitation;

«procédure de gestion des risques»: l'ensemble de la procédure consistant à identifier, contrôler et limiter les événements aléatoires susceptibles d'avoir des répercussions sur une organisation ou sur tout système qu'elle utilise. Elle couvre l'ensemble des activités liées aux risques, y compris l'évaluation, le traitement, l'acceptation et la communication;

«traitement des risques»: le fait d'atténuer, d'éliminer, de réduire (par un ensemble approprié de mesures sur le plan technique, physique ou au niveau de l'organisation ou des procédures), de transférer ou de surveiller les risques;

«annexe de sécurité (AS)»: un ensemble de conditions contractuelles spéciales, établi par l'autorité contractante, qui fait partie intégrante de tout contrat classifié impliquant l'accès à des ICUE ou la création de telles informations, dans lequel sont définis les conditions de sécurité ou les éléments du contrat qui doivent être protégés pour des raisons de sécurité — voir annexe A V, section II;

«guide de classification de sécurité» (GCS): un document qui décrit les éléments d'un programme ou d'un contrat qui sont classifiés, et précise les niveaux de classification de sécurité applicables. Le GCS peut être étoffé tout au long de la durée du programme ou du contrat et les éléments d'information peuvent être re-classifiés ou déclassés; lorsqu'il existe, le GCS fait partie de l'AS — voir annexe A V, section II;

«enquête de sécurité»: les procédures d'enquête menées par l'autorité compétente d'un État membre, dans le respect de ses dispositions législatives et réglementaires nationales, en vue d'obtenir l'assurance qu'il n'existe pas de renseignements défavorables de nature à empêcher une personne d'obtenir une HSP nationale ou de l'UE lui permettant d'avoir accès à des ICUE jusqu'à un niveau déterminé (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur);

«procédures d'exploitation de sécurité» (SecOPs): description des mesures de mises en œuvre de la politique de sécurité à adopter, des procédures d'exploitation à suivre et des responsabilités du personnel;

les «informations sensibles non classifiées»: à savoir toute information ou tout matériel que le SEAE est tenu de protéger en raison d'obligations légales énoncées dans les traités ou des actes adoptés en application de ces derniers, et/ou en raison de leur sensibilité. Les informations sensibles non classifiées incluent, mais sans s'y limiter, toute information ou tout matériel couvert par l'obligation de secret professionnel, telle que visée à l'article 339 du TFUE, toute information couverte par les intérêts protégés à l'article 4 du règlement (CE) nº 1049/2001 du Parlement européen et du Conseil ([1]), lu conjointement avec la jurisprudence correspondante de la Cour de justice de l'Union européenne, ou les données à caractère personnel entrant dans le champ d'application du règlement (CE) nº 45/2001.

«énoncé des impératifs de sécurité propres à un système» (SSRS): ensemble contraignant de principes de sécurité à respecter et d'impératifs de sécurité détaillés à mettre en œuvre, sous-tendant la procédure de certification et d'accréditation des SIC;

«TEMPEST»: l'analyse, l'étude et le contrôle des émissions électromagnétiques susceptibles de compromettre les informations, ainsi que les mesures destinées à les éliminer;

«menace»: la cause potentielle d'un incident non souhaité susceptible de porter atteinte à une organisation ou à tout système qu'elle utilise. Les menaces peuvent être accidentelles ou délibérées (malveillantes); elles sont caractérisées par des éléments menaçants, des cibles potentielles et des méthodes d'attaque;

«vulnérabilité»: toute faiblesse de quelque nature que ce soit dont une ou plusieurs menaces est susceptible de tirer parti pour se concrétiser. La vulnérabilité peut résulter d'une omission ou être liée à un contrôle défaillant en termes de rigueur, d'exhaustivité ou d'homogénéité; elle peut être de nature technique, procédurale, physique, organisationnelle ou opérationnelle.

([1]) Règlement (CE) nº 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (JO L 145 du 31.5.2001, p. 43).

Appendice B

Équivalence des classifications de sécurité

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL EU/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
EURATOM	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Belgique	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	note (1) ci-dessous
Bulgarie	Строго секретно	Секретно	Поверително	За служебно ползване
République tchèque	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danemark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Allemagne	STRENG GEHEIM	GEHEIM	VS (2) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Estonie	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irlande	Top Secret	Secret	Confidential	Restricted
Grèce	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Espagne	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSION LIMITADA
France	Très Secret Défense	Secret Défense	Confidentiel Défense	note (3) ci-dessous
Croatie	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italie	Segretissimo	Segreto	Riservatissimo	Riservato
Chypre	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Lettonie	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lituanie	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembourg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hongrie	«Szigorúan titkos!»	«Titkos!»	«Bizalmas!»	«Korlátozott terjesztésű!»
Malte	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Pays-Bas	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Autriche	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Pologne	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL EU/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Roumanie	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovénie	Strogo tajno	Tajno	Zaupno	Interno
Slovaquie	Prísne tajné	Tajné	Dôverné	Vyhradené
Finlande	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Suède (4)	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Royaume-Uni	UK TOP SECRET	UK SECRET	Pas d'équivalent (5)	UK OFFICIAL — SENSITIVE

(1) La classification «Diffusion restreinte/Beperkte Verspreiding» n'est pas une classification de sécurité en Belgique. La Belgique traite et protège les informations RESTREINT UE/EU RESTRICTED d'une manière qui n'est pas moins stricte que les normes et procédures décrites dans le règlement de sécurité du Conseil de l'Union européenne.

(2) Allemagne: VS = Verschlusssache.

(3) La France n'utilise pas la catégorie de classification «RESTREINT» dans son système national. Elle traite et protège les informations RESTREINT UE/EU RESTRICTED d'une manière qui n'est pas moins stricte que les normes et procédures décrites dans le règlement de sécurité du Conseil de l'Union européenne.

(4) Suède: les marquages de classification de sécurité de la première ligne sont utilisés par les autorités chargées de la défense et les marquages de la deuxième ligne par les autres autorités.

(5) Le Royaume-Uni traite et protège les ICUE marquées CONFIDENTIEL UE/EU CONFIDENTIAL conformément aux exigences de sécurité relatives à la protection des informations classifiées UK SECRET.

ISSN 1977-0936 (édition électronique)
ISSN 1725-2431 (édition papier)

Office des publications de l'Union européenne
2985 Luxembourg
LUXEMBOURG

FR