II

(Actes dont la publication n'est pas une condition de leur applicabilité)

CONSEIL

DÉCISION DU CONSEIL

du 19 mars 2001

adoptant le règlement de sécurité du Conseil

(2001/264/CE)

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité instituant la Communauté européenne, et notamment son article 207, paragraphe 3,

vu la décision 2000/396/CE, CECA, Euratom du Conseil du 5 juin 2000 portant adoption de son règlement intérieur [1], et notamment son article 24,

considérant ce qui suit:

(1) Afin de développer les activités du Conseil dans des domaines qui requièrent un certain degré de confidentialité, il convient de mettre en place un système de sécurité global concernant le Conseil, son Secrétariat général et les États membres.

(2) Ce système devrait regrouper dans un texte unique les matières visées par toutes les décisions et dispositions prises antérieurement dans ce domaine.

(3) En pratique, la majeure partie des informations de l'UE classifiées au niveau CONFIDENTIEL UE et au-delà concernera la politique commune en matière de sécurité et de défense.

(4) Afin d'assurer l'efficacité du système de sécurité ainsi créé, il y a lieu d'associer les États membres à son fonctionnement, en ce sens qu'ils doivent prendre les mesures nationales nécessaires pour assurer le respect des dispositions de la présente décision lorsque leurs autorités et leurs fonctionnaires compétents traitent des informations classifiées de l'UE.

(5) Le Conseil se félicite de l'intention qu'a la Commission d'instaurer, d'ici à la date d'application de la présente décision, un système global qui soit conforme aux annexes de la présente décision, afin d'assurer le bon fonctionnement du processus de décision au sein de l'Union.

(6) Le Conseil souligne combien il est important d'associer, le cas échéant, le Parlement européen et la Commission à la réglementation et aux normes de confidentialité qui sont nécessaires pour protéger les intérêts de l'Union et de ses États membres.

(7) La présente décision est arrêtée sans préjudice de l'article 255 du traité, ni des instruments le mettant en œuvre.

(8) La présente décision est arrêtée sans préjudice des pratiques en vigueur au sein des États membres en matière d'information de leurs parlements nationaux sur les activités de l'Union,

DÉCIDE:

Article premier

Le règlement de sécurité du Conseil figurant à l'annexe est approuvé.

Article 2

1. Le Secrétaire général/Haut représentant prend les mesures appropriées pour faire en sorte que, lors du traitement d'informations classifiées de l'UE, le règlement visé à l'article 1er soit respecté au sein du Secrétariat général du Conseil (ci-après dénommé «SGC») par les fonctionnaires et autres agents du SGC, les contractants extérieurs du SGC et le personnel détaché auprès du SGC, ainsi que dans les locaux du Conseil et au sein des organismes décentralisés de l'UE [2].

[1] JO L 149 du 23.6.2000, p. 21.

[2] Cf. conclusions du Conseil du 10 novembre 2000.

2. Les États membres prennent les mesures appropriées, conformément aux dispositions nationales, pour faire en sorte que, lors du traitement d'informations classifiées de l'UE, le règlement visé à l'article 1er soit respecté au sein de leurs services et dans leurs locaux par:

a) les membres des représentations permanentes des États membres auprès de l'Union européenne ainsi que par les membres des délégations nationales assistant à des réunions du Conseil ou de ses instances, ou participant à d'autres activités du Conseil;

b) les autres membres des administrations nationales des États membres qui traitent des informations classifiées de l'UE, qu'ils soient affectés sur le territoire des États membres ou à l'étranger;

c) les contractants extérieurs des États membres et le personnel détaché qui traitent des informations classifiées de l'UE.

Les États membres informent immédiatement le SGC de ces mesures.

3. Les mesures visées aux paragraphes 1 et 2 sont prises avant le 30 novembre 2001.

Article 3

Dans le respect des principes de base et des normes de sécurité minimales figurant dans la partie I de l'annexe, le Secrétaire général/Haut représentant peut prendre des mesures conformément à la partie II, section I, points 1 et 2, de l'annexe.

Article 4

À partir de sa date d'application, la présente décision remplace:

a) la décision 98/319/CE du Conseil du 27 avril 1998 relative aux modalités selon lesquelles les fonctionnaires et agents du Secrétariat général du Conseil peuvent être autorisés à avoir accès à des informations classifiées détenues par le Conseil [1];

b) la décision du Secrétaire général/Haut représentant du 27 juillet 2000 relative aux mesures de protection des informations classifiées applicables au Secrétariat général du Conseil [2];

c) la décision nº 433/97 du Secrétaire général du Conseil du 22 mai 1997 relative à la procédure d'habilitation des fonctionnaires chargés du fonctionnement du système Cortesy.

Article 5

1. La présente décision prend effet le jour de sa publication.

2. Elle s'applique à partir du 1er décembre 2001.

Fait à Bruxelles, le 19 mars 2001.

Par le Conseil
Le président
A. LINDH

[1] JO L 140 du 12.5.1998, p. 12.
[2] JO C 239 du 23.8.2000, p. 1.

ANNEXE

RÈGLEMENT DE SÉCURITÉ DU CONSEIL DE L'UNION EUROPÉENNE

SOMMAIRE

Page

Annexes

PARTIE I

PRINCIPES DE BASE ET NORMES DE SÉCURITÉ MINIMALES

INTRODUCTION

1. Le présent document définit les principes de base et les normes de sécurité minimales que le Conseil, le Secrétariat général du Conseil (ci-après dénommé «SGC»), les États membres ainsi que les organismes décentralisés de l'Union européenne (ci-après dénommés «organismes décentralisés de l'UE») doivent respecter comme il convient, de manière à assurer la sécurité et de sorte que chacun puisse avoir la certitude qu'une norme de protection commune est établie.

2. On entend par «informations classifiées de l'UE», tout matériel et toute information dont la divulgation non autorisée porterait atteinte à des degrés divers aux intérêts de l'UE, ou à ceux d'un ou plusieurs de ses États membres, que ces informations aient leur origine à l'intérieur de l'UE ou dans les États membres, des États tiers ou des organisations internationales.

3. Dans le présent règlement, on entend par:

   a) «document», toute lettre, note, compte rendu, rapport, mémorandum, signal/message, croquis, photographie, diapositive, film, carte, graphique, plan, cahier ou carnet, stencil, papier carbone, ruban de machine à écrire ou d'imprimante, bande magnétique, cassette, disque informatique, CD-ROM, ou autre support physique sur lequel des informations sont enregistrées;

   b) «matériel», les documents définis au point a) ci-dessus et tout élément d'équipement ou d'arme déjà fabriqué ou en cours de fabrication.

4. La sécurité a pour objectifs principaux:

   a) la sauvegarde des informations classifiées de l'UE contre l'espionnage, la compromission ou la divulgation non autorisée;

   b) la sauvegarde des informations de l'UE faisant l'objet de communications et transitant par des systèmes et réseaux d'information contre les menaces pesant sur leur intégrité et leur disponibilité;

   c) la sauvegarde des installations abritant des informations de l'UE contre les tentatives de sabotage et les actes intentionnels de détérioration;

   d) en cas d'échec, l'évaluation du dommage causé, la limitation de ses conséquences et l'adoption de mesures correctives nécessaires.

5. Un système de sécurité fiable a pour fondements:

   a) au sein de chaque État membre, une organisation nationale de sécurité qui assure:

      i) la collecte et l'enregistrement des données de renseignement concernant l'espionnage, le sabotage, le terrorisme ou d'autres activités subversives, et

      ii) la communication au gouvernement et, par l'intermédiaire de ce dernier, au Conseil, d'informations sur la nature des menaces qui pèsent sur la sécurité et de conseils sur les moyens de s'en protéger;

   b) au sein de chaque État membre et au sein du SGC, une autorité technique INFOSEC chargée de travailler avec l'autorité responsable de la sécurité concernée pour fournir des informations sur les menaces d'ordre technique pesant sur la sécurité et des conseils sur les moyens de s'en protéger;

   c) une collaboration régulière entre les services et agences officiels et les services compétents du SGC, pour déterminer:

      i) les informations, les ressources et les installations à protéger, et

      ii) les normes communes de protection

      et émettre, le cas échéant, des recommandations à ce sujet.

6. En matière de confidentialité, prudence et expérience sont nécessaires pour choisir les informations et matériels à protéger et évaluer le degré de protection à assurer. Celui-ci — et il s'agit là d'un aspect fondamental — doit être en rapport avec l'importance que revêtent, du point de vue de la sécurité, les informations et matériels à protéger. Afin d'assurer la bonne circulation des informations, des mesures doivent être prises pour éviter la surclassification. Le système de classification constitue l'instrument qui permet de mettre en œuvre ces principes; il conviendrait d'adopter un système similaire pour la planification et l'organisation des mesures de lutte contre l'espionnage, le sabotage, le terrorisme et d'autres menaces de façon à protéger au mieux les installations les plus importantes contenant des informations classifiées et, à l'intérieur de ces installations, les éléments les plus sensibles.

PRINCIPES DE BASE

7. **Les mesures de sécurité doivent:**

a) s'appliquer à toutes les personnes ayant accès à des informations classifiées, aux moyens de transmission des informations classifiées, à tous les locaux contenant de telles informations et aux installations importantes;

b) être conçues de façon à permettre de repérer les personnes dont l'emploi pourrait nuire à la sécurité des informations classifiées et des installations importantes contenant de telles informations, et de les exclure ou de les changer de poste;

c) empêcher toute personne non autorisée à avoir accès à des informations classifiées et aux installations qui en contiennent;

d) permettre de veiller à ce que la diffusion des informations classifiées repose exclusivement sur le principe du besoin d'en connaître, fondamental pour tous les aspects de la sécurité;

e) permettre d'assurer l'intégrité (c'est-à-dire empêcher l'altération, ou la modification ou la destruction non autorisées) et la disponibilité (c'est-à-dire que l'accès ne soit pas refusé aux personnes qui ont besoin de consulter les informations et qui y sont autorisées) de toutes les informations, classifiées ou non, et en particulier des informations stockées, traitées ou transmises par voie électromagnétique.

ORGANISATION DE LA SÉCURITÉ

Normes minimales communes

8. Le Conseil et chaque État membre doivent veiller à ce que tous les services administratifs et/ou officiels, les autres institutions, organismes et contractants de l'UE respectent les normes minimales communes en matière de sécurité, de sorte que l'on ait la certitude, au moment de communiquer une information classifiée de l'UE, qu'elle sera traitée par toutes ces instances avec les mêmes précautions. Ces normes minimales doivent comprendre les critères applicables à l'habilitation du personnel et les mesures à prendre pour la protection des informations classifiées de l'UE.

MESURES DE SÉCURITÉ RELATIVES AU PERSONNEL

Habilitations de sécurité

9. Toute personne devant avoir accès à des informations classifiées CONFIDENTIEL UE ou au-dessus, doit au préalable justifier d'une habilitation de sécurité appropriée. Une habilitation similaire est exigée pour les personnes dont les fonctions consistent à assurer l'exploitation et la maintenance technique de systèmes de communication et d'information contenant des informations classifiées. Cette habilitation devra permettre d'établir si:

a) la personne concernée est d'une loyauté à toute épreuve;

b) sa personnalité et sa discrétion sont telles que son intégrité ne puisse être mise en doute dès lors qu'elle aura accès à des informations classifiées;

c) elle est susceptible de céder aux pressions que pourraient exercer des sources étrangères ou autres, par exemple en raison de son lieu de résidence antérieur ou de contacts passés, qui pourraient constituer un risque pour la sécurité.

Une attention toute particulière devra être accordée au processus d'habilitation de personnes qui:

d) doivent avoir accès à des informations TRÈS SECRET UE/EU TOP SECRET;

e) occupent des postes nécessitant l'accès régulier à de nombreuses informations SECRET UE;

f) auxquelles leurs fonctions confèrent un accès spécial aux systèmes de communication ou d'information afférents à une mission essentielle et qui ont donc la possibilité d'accéder sans autorisation à un grand nombre d'informations classifiées de l'UE ou de compromettre gravement la mission par des actes de sabotage technique.

Dans les cas visés aux points d), e) et f), il faut faire appel au maximum aux méthodes d'enquête sur les antécédents.

10. Lorsqu'une personne n'ayant pas nécessairement le «besoin d'en connaître» doit être employée dans une fonction susceptible de lui donner accès à des informations classifiées de l'UE (par exemple, messager, agent de sécurité, personnel de maintenance ou de nettoyage), elle doit, au préalable, posséder l'habilitation appropriée.

Registres des habilitations de sécurité du personnel

11. Tout service, organisme ou établissement ayant à traiter des informations classifiées de l'UE ou hébergeant des systèmes de communication ou d'information indispensables à une mission doit tenir un registre des habilitations accordées à son personnel. Chaque habilitation doit être vérifiée, en fonction des circonstances, afin de s'assurer qu'elle est conforme aux niveaux de classification des informations et matériels que son bénéficiaire aura à traiter; une nouvelle vérification devient prioritaire chaque fois qu'une information nouvelle laisse à penser que le maintien de la personne concernée dans un poste donnant accès à des informations classifiées n'est plus compatible avec la sécurité. Le registre des habilitations est détenu par le responsable de la sécurité du service, de l'organisme ou de l'établissement concerné.

Formation du personnel dans le domaine de la sécurité

12. Toute personne occupant un poste qui peut lui donner accès à des informations classifiées doit recevoir, lors de son entrée en fonction puis à intervalles réguliers, un exposé très complet des mesures de sécurité nécessaires et des procédures en vigueur à cet égard. Il est utile d'exiger de tous ces membres du personnel qu'ils certifient par écrit avoir pleinement compris les règles de sécurité applicables à leur poste.

Responsabilités du personnel d'encadrement

13. Il incombe au personnel d'encadrement de savoir quels sont les membres du personnel qui traitent des informations classifiées ou qui ont accès à des systèmes de communication ou d'information afférents à une mission essentielle, de prendre note des incidents ou vulnérabilités manifestes pouvant avoir des répercussions sur le plan de la sécurité, et de les signaler.

Statut du personnel en matière de sécurité

14. Il convient d'établir des procédures permettant, si des renseignements défavorables viennent à être communiqués à propos d'une personne donnée, de déterminer si cette personne occupe une fonction nécessitant l'accès à des informations classifiées, ou si elle a accès à des systèmes de communication ou d'information afférents à une mission essentielle, et d'informer les autorités compétentes. S'il s'avère que cette personne présente un risque pour la sécurité, elle doit être renvoyée ou écartée des fonctions dans lesquelles elle risquerait de nuire à la sécurité.

MESURES PHYSIQUES DE SÉCURITÉ

Exigences en matière de protection

15. Le degré de sécurité physique à mettre en œuvre pour assurer la protection des informations classifiées de l'UE doit être proportionnel à la classification des informations et matériels détenus et à leur volume, ainsi qu'à la menace à laquelle ils sont exposés. Il convient donc d'éviter à la fois la surclassification et la sous-classification et de revoir périodiquement la classification attribuée. Tous les détenteurs d'informations classifiées de l'UE doivent se conformer à des règles normalisées de classification et respecter des critères de protection communs concernant la garde, la transmission et la destruction d'informations et matériels devant être protégés.

Contrôles

16. Avant de laisser sans surveillance un secteur contenant des informations classifiées de l'UE, les personnes en ayant la garde doivent s'assurer qu'elles sont en sécurité et que tous les dispositifs de sécurité (fermetures, alarmes, etc.) sont enclenchés. Des contrôles supplémentaires doivent être effectués par d'autres agents en dehors des heures de bureau.

Sécurité des bâtiments

17. Les bâtiments contenant des informations classifiées de l'UE ou des systèmes de communication et d'information indispensables à une mission doivent être protégés contre l'accès des personnes non autorisées. La nature de cette protection (par exemple fenêtres à barreaux, portes verrouillables, présence de gardes aux entrées, systèmes de contrôle d'entrée automatiques, inspections et patrouilles de sécurité, systèmes d'alarme, systèmes de détection des intrusions et chiens de garde) est fonction des paramètres suivants:

a) classification, volume et localisation dans le bâtiment concerné des informations et matériels à protéger;

b) qualité des meubles de sécurité contenant ces informations et matériels;

c) caractéristiques techniques et situation du bâtiment.

18. De même, la nature de la protection accordée aux systèmes de communication et d'information est fonction de l'évaluation de la valeur des informations et matériels en jeu et des dommages potentiels en cas de compromission de la sécurité, des caractéristiques techniques et de la situation du bâtiment qui héberge le système concerné, ainsi que de la localisation du système dans le bâtiment.

Plans d'urgence

19. Il faut établir à l'avance des plans détaillés, destinés à protéger les informations classifiées en cas d'urgence liée à la situation locale ou nationale.

SÉCURITÉ DES SYSTÈMES D'INFORMATION (INFOSEC)

20. La sécurité des systèmes d'information (INFOSEC) a trait à la détermination et à l'application des mesures de sécurité permettant de protéger les informations traitées, stockées ou transmises par des systèmes de communication, d'information et autres systèmes électroniques contre les atteintes à la confidentialité, à l'intégrité ou à la disponibilité de ces informations, que celles-ci soient accidentelles ou intentionnelles. Il convient de prendre des mesures préventives appropriées afin d'empêcher que des utilisateurs non autorisés accèdent aux informations de l'UE, que des utilisateurs autorisés se voient refuser l'accès à ces informations et d'empêcher l'altération, la modification ou la destruction non autorisées des informations de l'UE.

PROTECTION CONTRE LE SABOTAGE OU TOUT AUTRE ACTE INTENTIONNEL DE DÉTÉRIORATION

21. Les précautions physiques sont le moyen le plus efficace d'assurer la sécurité et la protection des installations importantes qui contiennent des informations classifiées contre le sabotage ou tout autre acte intentionnel de détérioration; la seule habilitation du personnel ne saurait s'y substituer efficacement. C'est à l'organisme national responsable de la sécurité qu'il incombe de rassembler les renseignements ayant trait à des activités d'espionnage, de sabotage, de terrorisme et à d'autres activités subversives.

COMMUNICATION D'INFORMATIONS CLASSIFIÉES À DES ÉTATS TIERS OU À DES ORGANISATIONS INTERNATIONALES

22. Il appartient au Conseil d'autoriser la communication d'informations classifiées de l'UE émanant du Conseil à un État tiers ou à une organisation internationale. Si l'autorité d'origine des informations à communiquer n'est pas le Conseil, ce dernier doit au préalable lui demander son consentement. Au cas où l'auteur ne peut être identifié, le Conseil en assume la responsabilité.

23. Si le Conseil reçoit des informations classifiées d'États tiers, d'organisations internationales ou d'autres tiers, il leur sera donné la protection conforme à leur classification et correspondant aux normes prévues par le présent règlement pour les informations classifiées de l'UE, ou aux normes plus strictes qui pourraient être exigées par le tiers qui communique ces informations. Des contrôles réciproques peuvent être prévus.

24. Les principes susmentionnés sont appliqués conformément aux dispositions détaillées figurant dans la partie II.

PARTIE II

SECTION I

ORGANISATION DE LA SÉCURITÉ AU SEIN DU CONSEIL DE L'UNION EUROPÉENNE

Le Secrétaire général/Haut représentant

1. Le Secrétaire général/Haut représentant:

   a) applique la politique de sécurité du Conseil;

   b) examine les problèmes de sécurité qui lui sont soumis par le Conseil ou ses instances compétentes;

   c) examine les questions impliquant des changements dans la politique de sécurité du Conseil, en étroite liaison avec les autorités nationales de sécurité (ou autres autorités appropriées) des États membres (ci-après dénommées «ANS»). L'annexe 1 contient une liste de ces autorités.

2. Plus particulièrement, le Secrétaire général/Haut représentant a la responsabilité:

   a) de coordonner toutes les questions de sécurité liées aux activités du Conseil;

   b) de demander la création par chaque État membre d'un registre central TRÈS SECRET UE/EU TOP SECRET et d'en exiger, le cas échéant, la création dans les organismes décentralisés de l'UE;

   c) de demander aux ANS des États membres de fournir les habilitations de sécurité intéressant le personnel employé au SGC conformément à la section VI;

   d) d'enquêter ou de faire enquêter sur toute fuite concernant les informations classifiées de l'UE si, à première vue, les indices montrent qu'une telle fuite s'est produite au SGC ou dans l'un ou l'autre des organismes décentralisés de l'UE;

   e) de demander aux autorités de sécurité compétentes d'entreprendre une enquête lorsqu'une fuite concernant des informations classifiées de l'UE semble s'être produite en dehors du SGC ou des organismes décentralisés de l'UE et de coordonner les enquêtes lorsqu'elles impliquent plus d'une autorité de sécurité;

   f) d'examiner périodiquement, en collaboration et en accord avec les ANS concernées, les dispositions prises pour protéger les informations classifiées de l'UE dans les États membres;

   g) de rester en liaison étroite avec toutes les autorités de sécurité concernées afin d'arriver à une coordination globale de la sécurité;

   h) de réexaminer constamment l'organisation et les procédures de sécurité du Conseil et, le cas échéant, de préparer les recommandations qui s'imposent. À ce titre, il soumet à l'approbation du Conseil le plan d'inspection annuel préparé par le Bureau de sécurité du SGC.

Le comité de sécurité du Conseil

3. Un comité de sécurité est créé. Il est composé de représentants de l'ANS de chaque État membre. Il est présidé par le Secrétaire général/Haut représentant ou par son délégué. Des représentants des organismes décentralisés de l'UE peuvent également être invités à assister à ses réunions lorsque les questions traitées les concernent.

4. Le comité de sécurité se réunit sur instruction du Conseil, sur demande du Secrétaire général/Haut représentant ou d'une ANS. Le comité est compétent pour examiner et évaluer toutes les questions de sécurité liées aux travaux du Conseil et pour lui présenter des recommandations, le cas échéant. En ce qui concerne les activités du SGC, le comité est habilité à faire des recommandations au Secrétaire général/Haut représentant sur les questions de sécurité.

Bureau de sécurité du Secrétariat général du Conseil

5. Afin de s'acquitter des responsabilités visées aux points 1 et 2, le Secrétaire général/Haut représentant dispose du Bureau de sécurité du SGC pour coordonner, superviser et exécuter les mesures de sécurité.

6. Le chef du Bureau de sécurité est le principal conseiller du Secrétaire général/Haut représentant sur les problèmes de sécurité et il assure le secrétariat du comité de sécurité. À ce titre, il dirige les travaux d'actualisation de la réglementation de sécurité et il assure la coordination des mesures de sécurité avec les autorités compétentes des États membres et, le cas échéant, avec les organisations internationales liées au Conseil par des accords de sécurité. À cette fin, il joue le rôle d'officier de liaison.

7. Le chef du Bureau de sécurité du SGC est responsable de l'homologation des systèmes et réseaux TI au sein du SGC. Le chef du Bureau de sécurité du SGC et les ANS concernées décident conjointement, le cas échéant, de l'homologation des systèmes et des réseaux TI faisant intervenir le SGC, les États membres, les organismes décentralisés de l'UE et/ou des tiers (États ou organisations internationales).

Organismes décentralisés de l'UE

8. Chaque directeur d'un organisme décentralisé de l'UE est responsable de l'application des règles de sécurité dans son organisme. Normalement, il charge un membre de son personnel de lui rendre compte en cette matière. Cette personne est désignée comme responsable de la sécurité.

États membres

9. Chaque État membre désigne une ANS responsable de la sécurité des informations classifiées de l'UE [1].

10. Au sein de l'administration de chaque État membre, l'ANS a la responsabilité:

    a) d'assurer la sécurité des informations classifiées de l'UE détenues dans tous les services, organismes ou agences nationaux, publics et privés, en métropole et à l'étranger;

    b) d'autoriser la création de bureaux d'ordre TRÈS SECRET UE/EU TOP SECRET (ce pouvoir peut être délégué à l'agent contrôleur TRÈS SECRET UE/EU TOP SECRET d'un bureau d'ordre central);

    c) de procéder périodiquement à l'inspection des dispositions de sécurité destinées à assurer la protection des informations classifiées de l'UE;

    d) de veiller à ce que tout le personnel national, de même que les ressortissants étrangers employés dans des services, organismes ou agences nationaux, susceptibles d'avoir accès aux informations UE classifiées TRÈS SECRET UE/EU TOP SECRET, SECRET UE et CONFIDENTIEL UE, possède une habilitation;

    e) de mettre au point les plans de sécurité jugés nécessaires pour éviter que des informations classifiées de l'UE ne tombent dans des mains non autorisées.

Inspections de sécurité réciproques

11. Des inspections périodiques des dispositions prises pour la protection des informations classifiées de l'UE au sein du SGC et des Représentations permanentes des États membres auprès de l'Union européenne, ainsi que des locaux réservés aux États membres dans les bâtiments du Conseil, sont menées, conjointement et d'un commun accord, par le Bureau de sécurité du SGC et par l'ANS concernée [2].

12. Des inspections périodiques des dispositions prises pour la protection des informations classifiées de l'UE dans les organismes décentralisés de l'UE sont menées par le Bureau de sécurité du SGC ou, à la demande du Secrétaire général/Haut représentant, par l'ANS de l'État membre d'accueil.

---

[1] La liste des ANS responsables de la sécurité des informations classifiées de l'UE figure à l'annexe 1.

[2] Sans préjudice de la Convention de Vienne de 1961 sur les relations diplomatiques.

SECTION II

CLASSIFICATIONS ET TIMBRES

DEGRÉS DE CLASSIFICATION ([1])

Les informations sont classifiées selon les degrés suivants:

1. TRÈS SECRET UE/EU TOP SECRET: cette classification s'applique exclusivement aux 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.

2. SECRET UE: cette classification s'applique uniquement aux 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.

3. CONFIDENTIEL UE: cette classification s'applique aux 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.

4. RESTREINT UE: cette classification s'applique aux 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.

TIMBRES

5. Un timbre restrictif peut être utilisé pour préciser le domaine couvert par le document ou pour indiquer une diffusion particulière fondée sur le besoin d'en connaître.

6. Le timbre PESD est apposé sur les documents et copies relatifs à la sécurité et à la défense de l'Union ou de l'un ou de plusieurs de ses États membres, ou relatifs à la gestion militaire et non militaire des crises.

7. Certains documents spécifiques aux systèmes de technologies de l'information (TI) peuvent porter un timbre complémentaire entraînant des mesures de sécurité supplémentaires définies dans la réglementation appropriée.

APPOSITION DES CLASSIFICATIONS ET DES TIMBRES

8. La classification et les timbres sont apposés comme suit:

   a) sur les documents RESTREINT UE, par voie mécanique ou électronique;

   b) sur les documents CONFIDENTIEL UE, par voie mécanique et à la main ou par impression sur du papier portant un cachet pré-imprimé et enregistré;

   c) sur les documents SECRET UE et TRÈS SECRET UE/EU TOP SECRET par voie mécanique et à la main.

([1]) Un tableau comparatif des classifications de l'UE, de l'OTAN, de l'UEO et des États membres figure à l'annexe 2.

SECTION III

POLITIQUE EN MATIÈRE DE CLASSIFICATION

1. Les informations ne sont classifiées qu'en cas de besoin. La classification est clairement et correctement indiquée et ne subsiste qu'aussi longtemps que les informations doivent être protégées.

2. La classification des informations ainsi que tout déclassement ou déclassification ultérieurs [1] incombe à la seule autorité d'origine.

   Les fonctionnaires et autres agents du SGC classifient, déclassent ou déclassifient les informations sur instruction de leur directeur général ou en accord avec celui-ci.

3. Les procédures détaillées régissant le traitement des documents classifiés ont été conçues de façon à assurer à ces documents une protection adaptée aux informations qu'ils contiennent.

4. Le nombre de personnes autorisées à établir des documents TRÈS SECRET UE/EU TOP SECRET doit être réduit au strict minimum et leur nom figurer sur une liste dressée par le SGC, chaque État membre et, le cas échéant, par chaque organisme décentralisé de l'UE.

DÉTERMINATION DE LA CLASSIFICATION

5. La classification d'un document est déterminée par le degré de sensibilité de son contenu, conformément aux définitions données aux points 1 à 4 de la section II. Il importe que la classification soit utilisée à bon escient et avec modération. Cela vaut en particulier pour la classification TRÈS SECRET UE/EU TOP SECRET.

6. En déterminant la classification à attribuer à un document, l'autorité d'origine doit tenir compte des diverses règles susmentionnées en réfrénant toute tendance à la surclassification comme à la sous-classification.

   Si l'emploi d'une classification élevée peut sembler à première vue garantir une meilleure protection des documents, un recours systématique à la surclassification peut entraîner une perte de confiance à l'égard de la valeur du système de classification.

   Inversement, le désir d'éviter certaines contraintes de protection ne doit pas conduire à sous-classifier les documents.

   Un guide pratique de la classification figure à l'annexe 3.

7. Des pages, paragraphes, sections, annexes, appendices et pièces jointes d'un document donné peuvent nécessiter une classification différente et doivent alors porter la mention afférente. La classification du document lui-même est celle de sa partie portant la classification la plus élevée.

8. Les lettres ou notes d'envoi accompagnant des pièces jointes portent le plus haut degré de classification apparaissant dans ces dernières. L'autorité d'origine indique clairement leur degré de classification lorsqu'elles sont séparées de leurs pièces jointes.

DÉCLASSEMENT ET DÉCLASSIFICATION

9. Un document classifié UE ne peut être déclassé ou déclassifié qu'avec l'autorisation de l'autorité d'origine et, si nécessaire, après consultation des autres parties intéressées. Le déclassement ou la déclassification fait l'objet d'une confirmation écrite. Il incombe à l'institution, à l'État membre, au bureau, à l'organisation repreneuse ou à l'autorité supérieure d'origine d'informer ses destinataires du changement de classification, ces derniers étant à leur tour chargés d'en aviser les destinataires successifs auxquels ils ont fait suivre l'original ou une copie du document.

10. Si possible, l'autorité d'origine indique sur le document classifié la date ou un délai à partir duquel les informations qu'il contient pourront être déclassées ou déclassifiées. Sinon, elle réexamine la question tous les cinq ans au plus pour s'assurer que la classification initiale est nécessaire.

---

[1] Par déclassement («downgrading»), on entend une diminution du degré de la classification. Par déclassification («declassification»), on entend la suppression de toute mention de classification.

SECTION IV

SÉCURITÉ PHYSIQUE

GÉNÉRALITÉS

1. Le principal objectif des mesures physiques de sécurité est d'empêcher qu'une personne non autorisée ait accès aux informations et/ou aux matériels classifiés de l'UE.

EXIGENCES EN MATIÈRE DE SÉCURITÉ

2. Il convient de protéger, par des mesures physiques de sécurité appropriées, chaque local, zone, bâtiment, bureau, pièce, systèmes de communication et d'information, etc., où des informations et du matériel classifiés de l'UE sont conservés et/ou traités.

3. Pour déterminer le degré de sécurité physique à assurer, il convient de tenir compte de tous les facteurs pertinents, et notamment:

   a) de la classification des informations et/ou du matériel;

   b) du volume et de la forme (par exemple support papier ou support de données informatiques) des informations détenues;

   c) de l'évaluation locale de la menace que constituent les services de renseignement prenant pour cible l'UE, les États membres et/ou les autres institutions ou tiers détenant des informations classifiées de l'UE, à savoir les actes de sabotage, le terrorisme et les autres activités subversives et/ou criminelles.

4. Les mesures physiques de sécurité appliquées doivent être conçues pour:

   a) empêcher toute intrusion par la ruse ou par la force;

   b) décourager, empêcher et détecter les actes commis par du personnel déloyal (espion de l'intérieur);

   c) empêcher que des fonctionnaires et autres agents du SGC, des services officiels des États membres et/ou d'autres institutions ou tiers qui n'ont pas le besoin d'en connaître accèdent à des informations classifiées de l'UE.

MESURES PHYSIQUES DE SÉCURITÉ

Zones de sécurité

5. Les zones où sont traitées et conservées des informations CONFIDENTIEL UE ou d'un niveau de classification plus élevé doivent être traitées et conservées de façon à correspondre à l'une des catégories suivantes:

   a) zone de sécurité de catégorie I: zone dans laquelle des informations CONFIDENTIEL UE ou d'un niveau de classification plus élevé sont traitées et conservées de telle façon que le fait de pénétrer dans la zone équivaut en pratique à avoir accès à ces informations. Pour une telle zone, il faut:

      i) établir de façon précise un périmètre protégé dont toutes les entrées et sorties sont contrôlées;

      ii) mettre en place un système de contrôle des entrées ne laissant pénétrer que les personnes dûment habilitées et spécialement autorisées;

      iii) spécifier la classification des informations qui y sont conservées habituellement, c'est-à-dire auxquelles le fait de pénétrer dans la zone donne accès;

   b) zone de sécurité de catégorie II: zone dans laquelle des informations CONFIDENTIEL UE ou d'un niveau de classification plus élevé sont traitées et conservées de telle façon qu'elles peuvent être protégées par des contrôles internes empêchant toute personne non autorisée d'y avoir accès; il s'agit, par exemple, des locaux abritant des bureaux où sont traitées et conservées habituellement des informations CONFIDENTIEL UE ou d'un niveau de classification plus élevé. Pour une telle zone, il faut:

      i) établir de façon précise un périmètre protégé dont toutes les entrées et sorties sont contrôlées;

      ii) mettre en place un système de contrôle des entrées ne laissant pénétrer sans escorte que les personnes dûment habilitées et spécialement autorisées. Pour toutes les autres personnes, il convient de prévoir une escorte ou des contrôles équivalents les empêchant d'avoir accès aux informations classifiées de l'UE et de pénétrer dans des zones soumises à des inspections techniques de sécurité.

Les zones qui ne sont pas occupées 24 heures sur 24 par le personnel de service doivent être inspectées immédiatement après les heures normales de travail, en vue de s'assurer que les informations classifiées de l'UE sont protégées comme il convient.

Zone administrative

6. Une zone de sécurité de catégorie I ou II peut être entourée ou précédée d'une zone administrative moins protégée, pour laquelle il faut établir de façon visible un périmètre permettant de contrôler les personnes et les véhicules. Seules des informations RESTREINT UE peuvent être traitées et conservées dans les zones administratives.

Contrôle des entrées et des sorties

7. L'accès aux zones de sécurité des catégories I et II est contrôlé par un système de laissez-passer ou d'identification individuelle applicable au personnel permanent. Il faut également mettre sur pied un système de contrôle des visiteurs pour empêcher tout accès non autorisé à des informations classifiées de l'UE. Au système de laissez-passer peut s'ajouter un système d'identification automatique, qui doit alors être considéré comme un complément et non comme un substitut absolu des gardes. Une modification de l'évaluation de la menace peut entraîner un renforcement des mesures de contrôle des entrées et des sorties, par exemple à l'occasion de visites de personnalités de haut rang.

Rondes

8. En dehors des heures de travail normales, des rondes de surveillance doivent être effectuées dans les zones de sécurité des catégories I et II pour protéger les informations et les matériels de l'UE contre la compromission, l'endommagement ou la perte. La fréquence de ces rondes est déterminée en fonction des conditions locales, mais elles doivent avoir lieu toutes les deux heures environ.

Meubles de sécurité et chambres fortes

9. Les meubles de sécurité destinés à la conservation d'informations classifiées de l'UE se répartissent en trois catégories:

   — catégorie A: meubles agréés selon les normes nationales pour la conservation d'informations TRÈS SECRET UE/EU TOP SECRET dans une zone de sécurité de catégorie I ou II,

   — catégorie B: meubles agréés selon les normes nationales pour la conservation d'informations SECRET UE et CONFIDENTIEL UE dans une zone de sécurité de catégorie I ou II,

   — catégorie C: meubles de bureau agréés pour la conservation d'informations RESTREINT UE seulement.

10. Pour les chambres fortes installées dans une zone de sécurité de catégorie I ou II et pour toutes les zones de sécurité de catégorie I où des informations CONFIDENTIEL UE et d'un niveau de classification plus élevé sont conservées en rayonnage ou figurent sur des diagrammes, des cartes, etc., les murs, les planchers, les plafonds, les portes et les serrures doivent être homologués par une ANS comme offrant une protection équivalant à celle d'un meuble de sécurité de la catégorie agréée pour la conservation d'informations de la même classification.

Serrures

11. Les serrures des meubles de sécurité et des chambres fortes abritant des informations classifiées de l'UE doivent satisfaire aux normes suivantes:

   — groupe A: agréées selon les normes nationales pour les meubles de catégorie A,

   — groupe B: agréées selon les normes nationales pour les meubles de catégorie B,

   — groupe C: adaptées aux meubles de bureau de catégorie C seulement.

Contrôle des clés et combinaisons

12. Les clés des meubles de sécurité ne doivent pas être emmenées hors du bâtiment. Les combinaisons doivent être mémorisées par les personnes qui ont besoin de les connaître. Pour un usage en cas d'urgence, le responsable de la sécurité de l'organisme intéressé conserve les clés de rechange et le relevé de chaque combinaison, placé individuellement dans une enveloppe opaque scellée. Les clés, leurs doubles et les enveloppes renfermant les combinaisons sont conservés dans des meubles de sécurité séparés. Ces clés et ces combinaisons font l'objet d'une protection aussi rigoureuse que le matériel auquel elles donnent accès.

13. Le nombre des personnes ayant connaissance des combinaisons des meubles de sécurité doit être aussi limité que possible. Les combinaisons sont modifiées:

a) à la réception d'un nouveau meuble;

b) lors de tout changement de personnel;

c) en cas de compromission, réelle ou suspectée;

d) de préférence tous les six mois et au minimum tous les douze mois.

Dispositifs de détection des intrusions

14. Lorsque des systèmes d'alarme, des circuits fermés de télévision et d'autres dispositifs électriques sont utilisés pour protéger des informations classifiées de l'UE, des systèmes de secours doivent être prévus pour permettre leur fonctionnement permanent en cas de rupture de l'alimentation électrique principale. Il est, en outre, fondamental que tout défaut de fonctionnement ou toute tentative de neutralisation des systèmes précités déclenche une alarme ou soit signalé par tout autre moyen fiable au personnel de surveillance.

Matériels agréés

15. Les ANS, seules ou avec celles d'un autre pays, doivent tenir à jour, par type et par modèle, les listes des matériels de sécurité qu'elles ont agréés pour la protection directe ou indirecte des informations classifiées dans diverses circonstances et conditions qui auront été spécifiées. Le Bureau de sécurité du SGC doit tenir à jour une liste comparable, fondée, entre autres, sur les informations fournies par les ANS. Les organismes décentralisés de l'UE consultent le Bureau de sécurité du SGC et, le cas échéant, l'ANS de l'État membre qui les accueille avant d'acheter ces matériels.

Protection physique des photocopieuses et des télécopieurs

16. Les photocopieuses et les télécopieurs doivent faire l'objet de mesures de protection physiques suffisantes pour que seules les personnes autorisées puissent les utiliser et que tous les tirages classifiés soient dûment contrôlés.

PROTECTION CONTRE LES REGARDS OU L'ÉCOUTE

Protection contre les regards

17. Toutes les mesures nécessaires doivent être prises, de jour comme de nuit, pour s'assurer que les informations classifiées de l'UE ne puissent être vues même accidentellement par des personnes non autorisées.

Protection contre l'écoute

18. Les bureaux ou les zones dans lesquels on discute régulièrement d'informations classifiées SECRET UE et d'un niveau de classification plus élevé doivent être protégés contre les tentatives d'écoute passive et active quand le risque le justifie. L'évaluation du risque de telles tentatives incombe à l'autorité de sécurité compétente après consultation, au besoin, des ANS.

19. Pour déterminer les mesures de protection à prendre dans les locaux sensibles contre les écoutes passives (par exemple, insonorisation des murs, portes, planchers et plafonds, mesure des rayonnements compromettants) et contre les écoutes actives (par exemple, recherche de micros), le Bureau de sécurité du SGC peut demander l'aide des spécialistes des ANS. Les responsables de la sécurité des organismes décentralisés de l'UE peuvent demander que le Bureau de sécurité du SGC procède à des inspections techniques et/ou demander l'aide des spécialistes des ANS.

20. De même, lorsque les circonstances l'exigent, les équipements de télécommunications et le matériel de bureau électrique ou électronique de toute nature utilisés lors des réunions de niveau SECRET UE et au-dessus peuvent être vérifiés, sur demande du responsable de la sécurité compétent, par des spécialistes de la sécurité technique des ANS.

ZONES PROTÉGÉES DU POINT DE VUE TECHNIQUE

21. Certaines zones peuvent être désignées comme zones protégées du point de vue technique. Un contrôle spécial doit être effectué à l'entrée. Elles doivent être verrouillées selon une méthode agréée lorsqu'elles ne sont pas occupées et toutes les clés doivent être considérées comme clés de sécurité. Ces zones doivent faire l'objet d'inspections physiques à intervalles réguliers, ainsi qu'après l'entrée, réelle ou présumée, de personnel non autorisé.

22. Un inventaire détaillé des équipements et mobiliers doit être tenu, afin d'en suivre les mouvements. Aucun meuble ou matériel ne doit être introduit dans une telle zone avant d'avoir subi une inspection minutieuse, effectuée par du personnel de sécurité formé à cet effet et destinée à détecter d'éventuels dispositifs d'écoute. En règle générale, l'installation de lignes de communication dans les zones protégées du point de vue technique devrait être évitée.

SECTION V

RÈGLES GÉNÉRALES CONCERNANT LE PRINCIPE DU BESOIN D'EN CONNAÎTRE ET LES HABILITATIONS DE SÉCURITÉ

1. L'accès aux informations classifiées de l'UE n'est autorisé qu'aux personnes ayant le besoin d'en connaître pour l'exercice de leurs fonctions ou l'accomplissement de leur mission. L'accès aux informations TRÈS SECRET UE/EU TOP SECRET, SECRET UE et CONFIDENTIEL UE n'est autorisé qu'aux personnes en possession de l'habilitation de sécurité correspondante.

2. Le besoin d'en connaître est déterminé par le SGC, les organismes décentralisés de l'UE et le service de l'État membre dans lequel la personne concernée exerce ses fonctions, compte tenu des nécessités de ces dernières.

3. L'habilitation de sécurité est délivrée par l'employeur de l'agent selon les procédures applicables en la matière. En ce qui concerne les fonctionnaires et autres agents du SGC, la procédure d'habilitation de sécurité est prévue à la section VI.

   Elle se concrétise par la délivrance d'un «certificat de sécurité» précisant le niveau des informations classifiées auxquelles la personne habilitée peut avoir accès et la date de péremption de cette habilitation.

   Un certificat de sécurité d'un niveau donné peut donner accès aux informations classifiées d'un niveau moindre.

4. Les personnes autres que les fonctionnaires ou autres agents du SGC ou des États membres (les membres, fonctionnaires ou agents des institutions de l'UE, par exemple) avec lesquelles il peut être nécessaire d'examiner ou de consulter des informations classifiées de l'UE, doivent être en possession d'une habilitation de sécurité leur permettant d'accéder aux informations classifiées de l'UE et être informées de leurs responsabilités en matière de sécurité. La même règle s'applique, dans des conditions similaires, aux contractants extérieurs, aux experts ou aux consultants.

RÈGLES PARTICULIÈRES CONCERNANT L'ACCÈS AUX INFORMATIONS TRÈS SECRET UE/EU TOP SECRET

5. Toute personne ayant à connaître des informations TRÈS SECRET UE/EU TOP SECRET doit avoir fait l'objet, au préalable, d'une procédure d'habilitation permettant l'accès à ces informations.

6. Toute personne qui doit avoir accès aux informations TRÈS SECRET UE/EU TOP SECRET doit être nommément désignée par le chef du service auquel elle appartient et son nom doit être conservé dans le bureau d'ordre TRÈS SECRET UE/EU TOP SECRET approprié.

7. Toute personne autorisée à accéder à des informations TRÈS SECRET UE/EU TOP SECRET doit signer au préalable une attestation reconnaissant qu'elle a été instruite des procédures de sécurité du Conseil et qu'elle comprend parfaitement sa responsabilité particulière en ce qui concerne la protection des informations TRÈS SECRET UE/EU TOP SECRET ainsi que les conséquences prévues par la réglementation UE et les dispositions législatives ou administratives de son pays, lorsque des informations classifiées parviennent en des mains non autorisées, que ce soit à la suite d'une action délibérée ou d'une négligence.

8. En ce qui concerne les personnes ayant accès à des informations TRÈS SECRET UE/EU TOP SECRET lors de réunions, etc., l'agent contrôleur compétent du service ou de l'organisme dans lesquels elles sont employées doit avertir le service qui organise la réunion qu'elles sont autorisées à avoir accès aux informations TRÈS SECRET UE/EU TOP SECRET.

9. Les noms de toutes les personnes qui ne sont plus employées dans des postes nécessitant l'accès aux informations TRÈS SECRET UE/EU TOP SECRET doivent être rayés de la liste TRÈS SECRET UE/EU TOP SECRET. De plus, l'attention de toutes ces personnes doit être attirée à nouveau sur leurs responsabilités particulières quant à la protection des informations TRÈS SECRET UE/EU TOP SECRET. Elles doivent également signer une déclaration par laquelle elles s'engagent à ne pas utiliser ni divulguer des informations TRÈS SECRET UE/EU TOP SECRET dont elles ont eu connaissance.

RÈGLES PARTICULIÈRES CONCERNANT L'ACCÈS AUX INFORMATIONS CLASSIFIÉES SECRET UE ET CONFIDENTIEL UE

10. Toute personne ayant à connaître des informations SECRET UE ou CONFIDENTIEL UE doit avoir fait au préalable l'objet d'une procédure d'habilitation du niveau approprié.

11. Toute personne ayant à connaître des informations SECRET UE ou CONFIDENTIEL UE doit avoir connaissance des règles de sécurité appropriées et des conséquences de toute négligence.

12. En ce qui concerne les personnes ayant accès à des informations SECRET UE ou CONFIDENTIEL UE lors de réunions, etc., le responsable de la sécurité de l'organisme dans lequel la personne concernée est employée doit avertir le service qui organise la réunion qu'elle est autorisée à avoir accès à de telles informations.

RÈGLES PARTICULIÈRES CONCERNANT L'ACCÈS AUX INFORMATIONS RESTREINT UE

13. Toute personne ayant accès à des informations RESTREINT UE doit être avertie des présentes règles de sécurité et des conséquences de toute négligence.

MUTATIONS

14. Lors de la mutation de personnel affecté à un poste impliquant le traitement de documents classifiés de l'UE, le bureau d'ordre doit s'assurer que le transfert de cette documentation entre le fonctionnaire partant et le fonctionnaire suivant s'effectue réglementairement.

PRESCRIPTIONS PARTICULIÈRES

15. Il convient que les personnes devant avoir accès à des informations classifiées de l'UE soient averties dès leur prise de fonctions, puis périodiquement:

    a) des dangers que présentent pour la sécurité les conversations indiscrètes;

    b) des précautions à prendre dans les relations avec la presse;

    c) de la menace que constituent les activités des services de renseignement qui prennent pour cible l'UE et les États membres et qui s'intéressent aux informations classifiées et aux activités de l'UE;

    d) de l'obligation qui leur est faite de rendre compte immédiatement à l'autorité de sécurité compétente de toute démarche ou manœuvre pouvant laisser soupçonner une activité d'espionnage, ou de toute situation inhabituelle ayant trait à la sécurité.

16. Toutes les personnes normalement exposées à des contacts fréquents avec des représentants de pays dont les services de renseignement prennent pour cible l'UE et les États membres et s'intéressent aux informations classifiées et aux activités de l'UE sont informées des techniques dont on sait qu'elles sont utilisées par divers services de renseignement.

17. Il n'existe pas de règles de sécurité du Conseil pour les voyages effectués à titre privé, quelle qu'en soit la destination, par des membres du personnel habilités à accéder à des informations classifiées de l'UE. Les autorités de sécurité compétentes informeront, toutefois, les fonctionnaires et autres agents se trouvant sous leur responsabilité des règles applicables aux voyages qu'ils peuvent avoir à respecter. Il appartient aux responsables de la sécurité d'organiser à l'intention des membres du personnel des séances de rappel de ces prescriptions particulières.

SECTION VI

PROCÉDURE D'HABILITATION DE SÉCURITÉ APPLICABLE AUX FONCTIONNAIRES ET AUTRES AGENTS DU SGC

1. Seuls les fonctionnaires et autres agents du SGC ou les personnes travaillant au sein du SGC qui, en raison de leurs fonctions et pour des nécessités de service, ont besoin de prendre connaissance d'informations classifiées détenues par le Conseil ou de traiter ces dernières, ont accès à ces informations.

2. Pour pouvoir accéder aux informations classifiées «TRÈS SECRET UE/EU TOP SECRET», «SECRET UE» et «CONFIDENTIEL UE», les personnes visées au point 1 doivent avoir été autorisées à cet effet, conformément à la procédure visée aux points 4 et 5.

3. L'autorisation n'est délivrée qu'aux personnes qui ont fait l'objet d'une enquête de sécurité effectuée par les autorités nationales compétentes des États membres (ANS), selon les modalités prévues aux points 6 à 10.

4. L'autorité investie du pouvoir de nomination (AIPN) au sens de l'article 2, premier alinéa, du Statut du personnel, est chargée de l'octroi des autorisations visées aux points 1, 2 et 3.

   L'AIPN octroie l'autorisation après avoir recueilli l'avis des autorités nationales compétentes des États membres sur la base de l'enquête de sécurité effectuée conformément aux points 6 à 12.

5. L'autorisation, qui a une durée de validité de cinq ans, ne peut excéder la durée des fonctions qui en ont justifié l'octroi. Elle peut être renouvelée par l'AIPN conformément à la procédure visée au point 4.

   L'autorisation est retirée par l'AIPN lorsqu'elle estime que des motifs le justifient. Toute décision de retrait est notifiée à la personne concernée, qui peut demander à être entendue par l'AIPN, ainsi qu'à l'autorité nationale compétente.

6. L'enquête de sécurité a pour objet de s'assurer qu'il n'y a pas d'objections à ce que la personne puisse avoir accès aux informations classifiées détenues par le Conseil.

7. L'enquête de sécurité est effectuée, avec le concours de la personne concernée et à la demande de l'AIPN, par les autorités nationales compétentes de l'État membre dont la personne à autoriser est ressortissante. Dans le cas où la personne concernée réside sur le territoire d'un autre État membre, les autorités nationales concernées peuvent s'assurer de la coopération des autorités de l'État de résidence.

8. En vue de l'enquête, la personne concernée est tenue de remplir une notice individuelle d'information.

9. L'AIPN spécifie dans sa demande le type et le niveau de classification des informations que la personne concernée aura à connaître, de sorte que les autorités nationales compétentes puissent mener l'enquête et rendre un avis quant au niveau d'autorisation qu'il serait approprié d'accorder à la personne concernée.

10. Sont applicables pour l'ensemble du déroulement et des résultats de la procédure d'enquête de sécurité, les prescriptions et réglementations en vigueur en la matière dans l'État membre concerné, y compris celles relatives aux éventuelles voies de recours.

11. Lorsque les autorités nationales compétentes des États membres émettent un avis positif, l'AIPN peut octroyer l'autorisation à la personne concernée.

12. Lorsque les autorités nationales compétentes émettent un avis négatif, la personne concernée est informée du sens de cet avis et peut demander à être entendue par l'AIPN. L'AIPN peut, si elle le juge nécessaire, s'adresser aux autorités nationales compétentes afin de demander les éclaircissements complémentaires qu'elles sont en mesure de donner. En cas de confirmation de l'avis négatif, l'autorisation ne peut être accordée.

13. Toute personne autorisée au sens des points 4 et 5 reçoit, au moment de l'autorisation et par la suite à intervalles réguliers, les instructions qui s'imposent sur la protection des informations classifiées et sur la manière de l'assurer. Elle signe une déclaration confirmant qu'elle a reçu ces instructions et qu'elle s'engage à les respecter.

14. L'AIPN prend toute mesure nécessaire pour mettre en œuvre la présente section, notamment celle relative à la réglementation de l'accès à la liste des personnes autorisées.

15. À titre exceptionnel et en raison des nécessités du service, l'AIPN peut, après en avoir préalablement informé les autorités nationales compétentes et en l'absence de réactions de celles-ci dans un délai d'un mois, octroyer une autorisation à titre temporaire pour une période qui ne peut excéder six mois, en attendant le résultat de l'enquête visée au point 7.

16. Les autorisations provisoires et temporaires ainsi octroyées ne donnent pas accès aux informations TRÈS SECRET UE/EU TOP SECRET; l'accès à ces informations est réservé aux fonctionnaires qui ont effectivement fait l'objet d'une enquête de sécurité dont l'issue a été positive, conformément au point 7. En attendant les résultats de l'enquête de sécurité, les fonctionnaires qui doivent être habilités au niveau TRÈS SECRET UE/EU TOP SECRET, peuvent être autorisés temporairement et provisoirement, à accéder aux informations classifiées jusqu'au niveau SECRET UE inclus.

SECTION VII

PRÉPARATION, DIFFUSION, TRANSMISSION, ARCHIVAGE ET DESTRUCTION DES MATÉRIELS CLASSIFIÉS DE L'UE

Sommaire

Dispositions générales

La présente section détaille les mesures de préparation, diffusion, transmission, archivage et destruction des documents classifiés de l'UE tels que définis au point 3, sous a), des principes de base et normes de sécurité minimales figurant dans la partie I de la présente annexe. Elle doit servir de référence pour l'adaptation de ces mesures aux autres matériels classifiés de l'UE, selon leur type et au cas par cas.

Chapitre I

Préparation et diffusion des documents classifiés de l'UE

PRÉPARATION

1. Comme cela est indiqué dans la section II, les classifications ainsi que les timbres UE doivent apparaître au milieu du haut et du bas de chaque page, et chaque page doit être numérotée. Chaque document classifié de l'UE doit porter un numéro de référence ainsi qu'une date. Pour les documents TRÈS SECRET UE/EU TOP SECRET et SECRET UE, ce numéro de référence sera porté sur chaque page. S'ils doivent être diffusés en plusieurs exemplaires, chacun d'eux devra porter un numéro d'exemplaire qui figurera en première page, avec le nombre total de pages. La première page d'un document classifié CONFIDENTIEL UE et au-dessus doit donner la liste complète des annexes et pièces jointes.

2. Les documents classifiés CONFIDENTIEL UE et au-dessus ne peuvent être dactylographiés, traduits, stockés, photocopiés, enregistrés sur un support magnétique ou microfilmés que par des personnes habilitées à avoir accès aux informations classifiées de l'UE, au moins jusqu'à la catégorie de sécurité appropriée du document en cause, sauf cas particulier exposé au point 27 de la présente section.

   Les dispositions relatives à la production de documents classifiés à l'aide de moyens informatiques sont énoncées dans la section XI.

DIFFUSION

3. Les informations classifiées de l'UE ne doivent être diffusées qu'auprès des personnes qui ont besoin d'en connaître et qui ont l'habilitation de sécurité appropriée. La diffusion initiale doit être précisée par l'autorité d'origine.

4. La diffusion des documents TRÈS SECRET UE/EU TOP SECRET s'effectue par la voie des bureaux d'ordre TRÈS SECRET UE/EU TOP SECRET (voir section VIII). Dans le cas de messages TRÈS SECRET UE/EU TOP SECRET, le bureau d'ordre compétent peut autoriser le chef du centre de transmission à réaliser le nombre de copies correspondant à la liste des destinataires.

5. Les documents classifiés SECRET UE et d'une classification moindre peuvent être rediffusés par un destinataire initial vers d'autres destinataires en fonction du besoin d'en connaître. Toutefois, les autorités d'origine doivent indiquer clairement toutes les restrictions qu'elles entendent imposer. Chaque fois que de telles restrictions sont imposées, les destinataires ne peuvent procéder à une rediffusion qu'avec l'autorisation des autorités d'origine.

6. À l'arrivée ou au départ, tout document classifié CONFIDENTIEL UE et au-dessus doit faire l'objet d'un enregistrement par le bureau d'ordre de l'organisme. Les éléments à enregistrer (références, date et, le cas échéant, numéro d'exemplaire) doivent permettre d'identifier les documents et figurent sur un cahier d'enregistrement ou sur des supports informatiques spéciaux et protégés.

Chapitre II

Transmission/transport de documents classifiés de l'UE

CONDITIONNEMENT

7. Les documents classifiés CONFIDENTIEL UE et au-dessus doivent être transmis sous une double enveloppe, opaque et résistante. L'enveloppe intérieure doit être cachetée et porter la classification de sécurité UE appropriée ainsi que, si possible, la mention complète des fonctions et de l'adresse du destinataire.

8. Seul l'agent contrôleur du bureau d'ordre, ou son remplaçant, peut ouvrir l'enveloppe intérieure et accuser réception des documents qu'elle renferme, à moins que cette enveloppe n'ait un destinataire précis. Dans ce cas, le bureau d'ordre approprié devra enregistrer la réception de l'enveloppe et seule la personne à laquelle elle est adressée pourra ouvrir l'enveloppe intérieure et accuser réception des documents qu'elle contient.

9. Une formule de récépissé est placée dans l'enveloppe intérieure. Le récépissé, qui n'est pas classifié, doit donner la référence, la date et le numéro d'exemplaire du document, mais jamais son objet.

10. L'enveloppe intérieure est enfermée dans une enveloppe extérieure, laquelle porte un numéro d'expédition en vue des formalités de réception. En aucun cas, la classification de sécurité ne doit apparaître sur l'enveloppe extérieure.

11. Pour les documents classifiés CONFIDENTIEL UE et au-dessus, les courriers et les messagers reçoivent un accusé de réception correspondant au numéro d'expédition.

TRANSMISSION À L'INTÉRIEUR D'UN BÂTIMENT OU GROUPE DE BÂTIMENTS

12. À l'intérieur d'un même bâtiment ou groupe de bâtiments, les documents classifiés peuvent être transmis dans une seule enveloppe fermée avec pour seule mention le nom du destinataire, à condition que le transport soit effectué par une personne habilitée au niveau de classification des documents.

TRANSMISSION DE DOCUMENTS UE À L'INTÉRIEUR D'UN MÊME PAYS

13. La transmission des documents TRÈS SECRET UE/EU TOP SECRET à l'intérieur d'un même pays doit être effectuée exclusivement par un service officiel de messagers ou par des personnes autorisées à avoir accès aux informations TRÈS SECRET UE/EU TOP SECRET.

14. Chaque fois qu'il est fait appel à un messager pour le transport d'un document TRÈS SECRET UE/EU TOP SECRET hors des limites d'un bâtiment ou groupe de bâtiments, il convient d'appliquer les dispositions relatives au conditionnement et à la réception définies au présent chapitre. Les services de messagerie doivent disposer d'un personnel suffisant pour que les paquets contenant des documents TRÈS SECRET UE/EU TOP SECRET demeurent sous le contrôle direct et permanent d'un responsable.

15. Exceptionnellement, des documents TRÈS SECRET UE/EU TOP SECRET peuvent être transportés par des fonctionnaires autres que les messagers hors des limites d'un bâtiment ou groupe de bâtiments pour être utilisés localement lors de réunions ou de débats, sous réserve que:

    a) le porteur soit autorisé à avoir accès à ces documents TRÈS SECRET UE/EU TOP SECRET;

    b) le mode de transport soit conforme aux règles nationales en matière de transmission de documents nationaux TRÈS SECRET;

    c) le porteur ne se sépare en aucun cas des documents TRÈS SECRET UE/EU TOP SECRET qu'il transporte;

    d) des dispositions soient prises pour que la liste des documents ainsi transportés soit conservée par le bureau d'ordre TRÈS SECRET UE/EU TOP SECRET détenteur et notée sur un registre, afin de permettre une vérification lors du retour de ces documents.

16. La transmission de documents SECRET UE et CONFIDENTIEL UE à l'intérieur d'un même pays peut être effectuée soit par la poste si ce mode de transmission est autorisé par la réglementation en matière de sécurité du pays, et conformément à cette réglementation, soit par un service de messagers, soit par des personnes autorisées à avoir accès aux informations classifiées de l'UE.

17. Chaque État membre ou organisme décentralisé de l'UE doit élaborer des instructions relatives au transport individuel de documents classifiés de l'UE sur la base de cette réglementation. Il devra être demandé au porteur de lire et de signer ces instructions, lesquelles indiqueront en particulier qu'en aucun cas:

    a) le porteur ne peut se défaire des documents, à moins que leur garde ne soit assurée conformément aux prescriptions de la section IV;

    b) les documents ne peuvent être laissés sans surveillance dans les moyens de transport publics ou les véhicules personnels, ni dans les lieux publics tels que restaurants ou hôtels. Ils ne peuvent être ni déposés dans les coffres d'hôtels ni conservés sans surveillance dans les chambres d'hôtel;

    c) les documents ne peuvent être lus dans des lieux publics, par exemple dans un avion ou dans un train.

TRANSMISSION D'UN ÉTAT MEMBRE À UN AUTRE

18. Les matériels CONFIDENTIEL UE et d'une classification supérieure sont transmis d'un État membre à un autre par les services du courrier diplomatique ou militaire.

19. Toutefois, le transport par une personne de matériel classifié SECRET UE et CONFIDENTIEL UE peut être autorisé si les dispositions prises pour le transport permettent de garantir que les documents ne pourront tomber entre les mains d'une personne non autorisée.

20. Les ANS peuvent autoriser le transport par une personne lorsqu'on ne peut utiliser ni courrier diplomatique ni courrier militaire, ou lorsque leur utilisation se traduirait par un retard risquant de compromettre des opérations de l'UE et que le matériel est requis d'urgence par son destinataire. Chaque État membre rédigera des instructions portant sur le transport international par des personnes autres que les courriers diplomatiques ou militaires des matériels classifiés jusqu'au niveau SECRET UE inclus. Dans ces instructions, il sera exigé que:

a) le porteur ait l'habilitation de sécurité appropriée délivrée par les États membres;

b) tous les matériels ainsi transportés soient enregistrés dans le bureau ou bureau d'ordre approprié;

c) les paquets ou les sacs contenant des matériels UE portent un sceau officiel permettant d'empêcher ou de décourager une inspection de la douane, et des étiquettes d'identification indiquant la marche à suivre pour la personne qui les trouvera;

d) le porteur soit muni d'un certificat de courrier et/ou d'un ordre de mission admis par tous les États de l'UE, l'autorisant à transporter le paquet dûment identifié;

e) il ne soit traversé ni frontière ni territoire d'États non membres de l'UE en cas de transport par voie terrestre, à moins que ces États n'aient fourni de garantie spécifique à l'État expéditeur;

f) en ce qui concerne la destination, l'itinéraire et les moyens de transport, les dispositions relatives au voyage du porteur soient conformes à la réglementation UE ou, s'ils sont plus stricts, aux règlements nationaux;

g) le porteur ne se sépare pas des matériels, à moins que leur garde ne soit assurée conformément aux dispositions de sécurité figurant à la section IV;

h) les matériels ne soient pas laissés sans surveillance dans les moyens de transport publics ou les véhicules personnels, ni dans les lieux publics tels que restaurants ou hôtels. Ils ne peuvent être ni déposés dans les coffres d'hôtels ni conservés sans surveillance dans les chambres d'hôtel;

i) si les matériels transportés contiennent des documents, ceux-ci ne soient pas lus dans des lieux publics (par exemple, dans un avion, dans un train, etc.).

La personne chargée de transporter les matériels classifiés doit lire et signer des instructions de sécurité contenant au minimum les instructions ci-dessus et indiquant la procédure à suivre en cas d'urgence ou au cas où le paquet contenant les matériels classifiés ferait l'objet d'un contrôle de la part des autorités douanières ou de sécurité d'un aéroport.

TRANSMISSION DE DOCUMENTS RESTREINT UE

21. Aucune disposition spéciale n'est fixée concernant la transmission des documents RESTREINT UE; celle-ci doit cependant s'effectuer de manière à ce qu'ils ne puissent tomber entre les mains de personnes non autorisées.

SÉCURITÉ RELATIVE AUX COURRIERS

22. Tous les courriers et messagers utilisés pour le transport des documents SECRET UE et CONFIDENTIEL UE doivent avoir fait l'objet d'une habilitation de sécurité appropriée.

Chapitre III

Transmission par voie électrique et autres moyens techniques

23. Les mesures de sécurité des télécommunications sont conçues pour assurer la transmission en toute sécurité des informations classifiées de l'UE. Les règles à observer lors de la transmission d'informations classifiées de l'UE figurent en détail à la section XI.

24. Seuls les centres et réseaux de transmissions et/ou les terminaux et systèmes homologués peuvent transmettre des informations CONFIDENTIEL UE et SECRET UE.

Chapitre IV

Exemplaires supplémentaires et traductions et extraits de documents classifiés de l'UE

25. Seule l'autorité d'origine peut autoriser la duplication ou la traduction de documents TRÈS SECRET UE/EU TOP SECRET.

26. Si des personnes ne possédant pas l'habilitation TRÈS SECRET UE/EU TOP SECRET ont besoin d'informations contenues dans un document TRÈS SECRET UE/EU TOP SECRET mais n'ont pas elles-mêmes ce niveau de classification, le chef du bureau d'ordre TRÈS SECRET UE/EU TOP SECRET peut être autorisé à réaliser le nombre d'extraits nécessaires de ce document. Il prendra en même temps les mesures requises pour que ces documents reçoivent une classification de sécurité appropriée.

27. Les reproductions et traductions de documents SECRET UE et d'une classification moindre peuvent être faites par le destinataire, dans le cadre des règlements de sécurité nationaux et à condition qu'il observe strictement le principe du besoin d'en connaître. Les mesures de sécurité applicables au document original le sont également à ses reproductions et/ou traductions. Les organismes décentralisés de l'UE doivent se conformer au présent règlement de sécurité.

Chapitre V

Inventaires et contrôles, archivage et destruction des documents classifiés de l'UE

INVENTAIRES ET CONTRÔLES

28. Tous les ans, chaque bureau d'ordre TRÈS SECRET UE/EU TOP SECRET visé à la section VIII procède à un inventaire détaillé des documents TRÈS SECRET UE/EU TOP SECRET conformément aux règles énoncées à la section VIII, points 9 à 11. Les documents classifiés de l'UE d'un niveau inférieur à TRÈS SECRET UE/EU TOP SECRET doivent faire l'objet de vérifications internes conformément aux directives nationales et, en ce qui concerne le SGC ou les organismes décentralisés de l'UE, conformément aux directives du Secrétaire général/Haut représentant.

Ces opérations permettent notamment de recueillir l'avis des détenteurs sur:

a) le déclassement ou la déclassification éventuels de certains documents;

b) les destructions à entreprendre.

ARCHIVAGE D'INFORMATIONS CLASSIFIÉES DE L'UE

29. Afin de limiter les problèmes d'archivage, les agents contrôleurs de tous les bureaux d'ordre sont autorisés à faire microfilmer les documents TRÈS SECRET UE/EU TOP SECRET, SECRET UE et CONFIDENTIEL UE, ou à les faire enregistrer sur un support magnétique ou optique à des fins d'archivage, à condition que:

a) les microfilms/l'archivage soient réalisés par des personnes possédant une habilitation correspondant à la classification appropriée, en cours de validité;

b) les microfilms/l'enregistrement bénéficient de la même sécurité que les documents originaux;

c) la mise sur microfilm/l'archivage d'un document TRÈS SECRET UE/EU TOP SECRET soit signalé(e) à l'autorité d'origine;

d) les rouleaux de films ou autres types de support ne contiennent que des documents d'une même classification TRÈS SECRET UE/EU TOP SECRET, SECRET UE ou CONFIDENTIEL UE;

e) la mise sur microfilm/l'archivage d'un document TRÈS SECRET UE/EU TOP SECRET ou SECRET UE soit clairement indiqué(e) sur le registre utilisé pour l'inventaire annuel;

f) les documents originaux qui ont été microfilmés ou archivés sur un autre support soient détruits, conformément aux règles énoncées aux points 31 à 36.

30. Ces règles s'appliquent également à tout autre moyen d'archivage autorisé par les ANS, tels que le support électromagnétique et le disque optique.

DESTRUCTION PÉRIODIQUE DE DOCUMENTS CLASSIFIÉS DE L'UE

31. Afin d'éviter l'accumulation inutile de documents classifiés de l'UE, ceux qui sont jugés périmés et excédentaires par le chef de l'organisme qui les détient doivent être détruits dès que possible, selon les modalités ci-après:

a) les documents TRÈS SECRET UE/EU TOP SECRET sont détruits uniquement par le bureau d'ordre central qui en a la charge. Chaque document détruit est inscrit sur un procès-verbal de destruction, signé par l'officier contrôleur TRÈS SECRET UE/EU TOP SECRET et par un témoin qui doit être habilité TRÈS SECRET UE/EU TOP SECRET. Le cahier d'enregistrement doit comporter une note à cet effet;

b) le bureau d'ordre doit conserver pendant dix ans les procès-verbaux de destruction, ainsi que les fiches de circulation. Des copies ne sont transmises à l'autorité d'origine ou au bureau d'ordre central approprié que sur demande expresse;

c) les documents TRÈS SECRET UE/EU TOP SECRET, y compris tous les rebuts classifiés résultant de l'élaboration de ces documents (exemplaires endommagés, brouillons, notes dactylographiées, papiers carbones, etc.), doivent être détruits sous la surveillance d'un responsable habilité TRÈS SECRET UE/EU TOP SECRET, par incinération, réduction en pulpe, lacération en bandes ou division en fragments non identifiables rendant impossible toute reconstitution.

32. Les documents SECRET UE doivent être détruits par le bureau d'ordre qui en a la charge, sous la surveillance d'une personne habilitée, et par l'un des procédés indiqués au point 31, sous c). La destruction de documents SECRET UE fait l'objet de procès-verbaux signés, conservés par le bureau d'ordre, avec les fiches de circulation, pendant au moins trois ans.

33. Les documents CONFIDENTIEL UE doivent être détruits par le bureau d'ordre qui en a la charge, sous la surveillance d'une personne habilitée, et par l'un des procédés indiqués au point 31, sous c). Leur destruction est enregistrée conformément aux réglementations nationales et, dans le cas du SGC ou des organismes décentralisés de l'UE, selon les directives du Secrétaire général/Haut représentant.

34. Les documents RESTREINT UE doivent être détruits par le bureau d'ordre qui en a la charge ou par l'utilisateur, conformément aux réglementations nationales et, dans le cas du SGC ou des organismes décentralisés de l'UE, selon les directives du Secrétaire général/Haut représentant.

DESTRUCTION EN CAS D'URGENCE

35. Le SGC, les États membres et les organismes décentralisés de l'UE établissent des plans tenant compte des conditions locales pour assurer la sauvegarde en temps de crise des matériels classifiés de l'UE, y compris si nécessaire des plans de destruction et d'évacuation en cas d'urgence; ils promulguent, dans leurs organisations respectives, les instructions jugées nécessaires pour éviter que des informations classifiées de l'UE ne tombent dans des mains non autorisées.

36. Les dispositions prises pour la sauvegarde et/ou la destruction en temps de crise des matériels SECRET UE et CONFIDENTIEL UE ne doivent en aucun cas nuire à la sauvegarde ni à la destruction des matériels TRÈS SECRET UE/EU TOP SECRET, et notamment des matériels de chiffrement, dont le traitement doit avoir la priorité sur toutes les autres tâches. Les mesures à prendre pour la sauvegarde et la destruction d'urgence des matériels de chiffrement font l'objet d'instructions ad hoc.

Chapitre VI

Règles particulières applicables aux documents destinés au Conseil

37. Au sein du SGC, un «bureau des informations classifiées» assure le suivi des informations classifiées SECRET UE et CONFIDENTIEL UE lorsqu'elles font l'objet de documents du Conseil.

Sous l'autorité du directeur général du personnel et de l'administration:

a) il gère les opérations relatives à leur enregistrement, reproduction, traduction, transmission, expédition et destruction;

b) il tient à jour le registre concernant les informations classifiées;

c) il interroge périodiquement les émetteurs sur la nécessité de maintenir la classification de ces informations;

d) il fixe, en concertation avec le Bureau de sécurité, les modalités pratiques pour la classification et la déclassification des informations.

38. Le bureau des informations classifiées tient un registre comportant les données suivantes:

a) la date de l'établissement de l'information classifiée;

b) le degré de la classification;

c) l'échéance de la classification;

d) le nom et le service de l'émetteur;

e) le ou les destinataires, avec indication du numéro d'ordre;

f) le sujet;

g) le numéro;

h) le nombre d'exemplaires diffusés;

i) l'élaboration d'inventaires des informations classifiées soumises au Conseil;

j) un registre où sont inscrites les opérations de déclassification et de déclassement des informations classifiées.

39. Les règles générales énoncées aux chapitres I à V de la présente section s'appliquent au bureau des informations classifiées du SGC, sauf modification par les règles particulières énoncées dans le présent chapitre.

SECTION VIII

BUREAUX D'ORDRE TRÈS SECRET UE/EU TOP SECRET

1. Le rôle d'un bureau d'ordre TRÈS SECRET UE/EU TOP SECRET est d'assurer l'enregistrement, le traitement et la diffusion des documents TRÈS SECRET UE/EU TOP SECRET conformément aux règles de sécurité. Le chef du bureau d'ordre TRÈS SECRET UE/EU TOP SECRET est respectivement dans chaque État membre, au sein du SGC et, le cas échéant, au sein des organismes décentralisés de l'UE, l'agent contrôleur TRÈS SECRET UE/EU TOP SECRET.

2. Les bureaux d'ordre centraux représentent la principale autorité de réception et de diffusion pour les États membres, le SGC et pour les organismes décentralisés de l'UE dans lesquels ils ont été créés, ainsi que, le cas échéant, pour les autres institutions de l'UE, les organisations internationales et les États tiers avec lesquels le Conseil a conclu des accords sur les procédures de sécurité pour l'échange d'informations classifiées.

3. En tant que de besoin, des bureaux d'ordre subordonnés sont créés afin d'assurer la gestion interne des documents TRÈS SECRET UE/EU TOP SECRET; ils tiennent à jour la situation de chacun des documents dont ils ont la charge.

4. Les bureaux d'ordre TRÈS SECRET UE/EU TOP SECRET subordonnés sont créés comme indiqué à la section I pour répondre à un besoin permanent et sont rattachés à un bureau d'ordre TRÈS SECRET UE/EU TOP SECRET central. S'il n'existe qu'un besoin de consultation temporaire et occasionnel de documents TRÈS SECRET UE/EU TOP SECRET, ces documents peuvent être communiqués sans création d'un bureau d'ordre TRÈS SECRET UE/EU TOP SECRET subordonné, sous réserve que les règles établies garantissent qu'ils resteront sous le contrôle du bureau d'ordre TRÈS SECRET UE/EU TOP SECRET approprié, et sous réserve du respect de toutes les mesures de sécurité physiques et concernant le personnel.

5. Les bureaux d'ordre subordonnés ne peuvent transmettre des documents TRÈS SECRET UE/EU TOP SECRET directement à d'autres bureaux d'ordre subordonnés au même bureau d'ordre TRÈS SECRET UE/EU TOP SECRET central sans l'autorisation expresse de ce dernier.

6. Tous les échanges de documents TRÈS SECRET UE/EU TOP SECRET entre des bureaux d'ordre subordonnés à des bureaux d'ordre centraux différents doivent transiter par les bureaux d'ordre TRÈS SECRET UE/EU TOP SECRET centraux.

BUREAUX D'ORDRE TRÈS SECRET UE/EU TOP SECRET CENTRAUX

7. En tant qu'agent contrôleur, le chef d'un bureau d'ordre TRÈS SECRET UE/EU TOP SECRET central a pour responsabilités:

   a) d'assurer la transmission des documents TRÈS SECRET UE/EU TOP SECRET conformément aux règles définies dans la section VII;

   b) de tenir à jour la liste de tous ses bureaux d'ordre TRÈS SECRET UE/EU TOP SECRET subordonnés avec les noms et les signatures des agents contrôleurs désignés et de leurs adjoints autorisés;

   c) de détenir les récépissés des bureaux d'ordre pour tous les documents TRÈS SECRET UE/EU TOP SECRET diffusés par le bureau d'ordre central;

   d) de tenir un état des documents TRÈS SECRET UE/EU TOP SECRET détenus et diffusés;

   e) de tenir à jour la liste de tous les bureaux d'ordre centraux TRÈS SECRET UE/EU TOP SECRET avec lesquels il correspond normalement, avec les noms et signatures des agents contrôleurs désignés et de leurs adjoints autorisés;

   f) d'assurer la sécurité matérielle de tous les documents TRÈS SECRET UE/EU TOP SECRET détenus dans le bureau d'ordre, conformément aux prescriptions énoncées dans la section IV.

BUREAUX D'ORDRE TRÈS SECRET UE/EU TOP SECRET SUBORDONNÉS

8. En tant qu'agent contrôleur, le chef d'un bureau d'ordre TRÈS SECRET UE/EU TOP SECRET subordonné a pour responsabilités:

   a) d'assurer la transmission des documents TRÈS SECRET UE/EU TOP SECRET conformément aux dispositions définies dans la section VII et aux points 5 et 6 de la section VIII;

b) de tenir à jour la liste de toutes les personnes autorisées à avoir accès aux informations TRÈS SECRET UE/EU TOP SECRET sous son contrôle;

c) de diffuser les documents TRÈS SECRET UE/EU TOP SECRET conformément aux instructions de l'autorité d'origine ou en fonction du besoin d'en connaître, en s'assurant, au préalable, que le destinataire possède une habilitation de sécurité du niveau requis;

d) de tenir à jour la liste de tous les documents TRÈS SECRET UE/EU TOP SECRET détenus ou en circulation sous son contrôle, ou qui ont été transmis à d'autres bureaux d'ordre TRÈS SECRET UE/EU TOP SECRET, et de détenir tous les récépissés correspondants;

e) de tenir à jour la liste des bureaux d'ordre TRÈS SECRET UE/EU TOP SECRET avec lesquels il est autorisé à échanger des documents TRÈS SECRET UE/EU TOP SECRET, ainsi que les noms et signatures des agents contrôleurs désignés et de leurs adjoints autorisés;

f) d'assurer la sécurité matérielle de tous les documents TRÈS SECRET UE/EU TOP SECRET conservés dans le bureau d'ordre subordonné conformément aux prescriptions énoncées dans la section IV.

INVENTAIRES

9. Tous les douze mois, chaque bureau d'ordre TRÈS SECRET UE/EU TOP SECRET procède à un inventaire détaillé de tous les documents TRÈS SECRET UE/EU TOP SECRET dont il est responsable. Un document est considéré comme comptabilisé par le bureau d'ordre si celui-ci a pu constater de visu son existence, ou détient soit un récépissé du bureau d'ordre TRÈS SECRET UE/EU TOP SECRET auquel il a été transmis, soit un procès-verbal de destruction du document, soit un ordre de déclassement ou de déclassification.

10. Les bureaux d'ordre subordonnés adressent au bureau d'ordre central dont ils relèvent, à la date fixée par ce dernier, les résultats de leur inventaire annuel.

11. Les ANS, ainsi que les institutions de l'UE, les organisations internationales et les organismes décentralisés de l'UE dans lesquels un bureau d'ordre TRÈS SECRET UE/EU TOP SECRET central a été créé, rendent compte au Secrétaire général/Haut représentant, au plus tard le 1er avril de chaque année, des résultats des inventaires annuels effectués dans les bureaux d'ordre TRÈS SECRET UE/EU TOP SECRET centraux.

SECTION IX

MESURES DE SÉCURITÉ À APPLIQUER À L'OCCASION DES RÉUNIONS SPÉCIFIQUES TENUES EN DEHORS DES LOCAUX DU CONSEIL ET PORTANT SUR DES DOSSIERS TRÈS SENSIBLES

GÉNÉRALITÉS

1. Les mesures de sécurité décrites ci-après doivent être prises lorsque les réunions du Conseil européen, les sessions du Conseil, les réunions ministérielles et autres réunions importantes ont lieu en dehors des locaux du Conseil à Bruxelles ou à Luxembourg, et lorsque les exigences de sécurité particulières découlant du niveau de sensibilité élevé des dossiers ou informations traités le justifient. Ces mesures ne concernent que la protection des informations classifiées de l'UE; il peut se révéler nécessaire de prévoir d'autres mesures de sécurité.

RESPONSABILITÉS

État membre d'accueil

2. L'État membre sur le territoire duquel se déroule la réunion (État membre d'accueil) doit assurer, en coopération avec le Bureau de sécurité du SGC, la sécurité du Conseil européen, de la session du Conseil, de la réunion ministérielle ou autre réunion importante, ainsi que la sécurité physique des principaux délégués et de leurs collaborateurs.

En matière de protection de la sécurité, l'État membre d'accueil doit en particulier veiller à ce que:

a) des plans soient établis pour faire face aux menaces pesant sur la sécurité et aux incidents en rapport avec cette dernière, les mesures prévues devant concerner notamment la protection des documents classifiés de l'UE à l'intérieur des locaux;

b) des dispositions soient prises afin d'assurer l'accès éventuel au système de télécommunication du Conseil pour la réception et l'envoi de messages classifiés de l'UE. L'État membre d'accueil veillera également à assurer, le cas échéant, l'accès à des systèmes téléphoniques protégés.

États membres

3. Les autorités des États membres font en sorte que:

a) les attestations d'habilitation de sécurité appropriées soient fournies pour leurs délégués nationaux, si nécessaire par message ou télécopie, soit directement au responsable de la sécurité de la réunion, soit par l'intermédiaire du Bureau de sécurité du SGC;

b) toute menace spécifique soit signalée aux autorités de l'État membre d'accueil et, le cas échéant, au Bureau de sécurité du SGC, afin que des mesures appropriées puissent être prises.

Responsable de la sécurité de la réunion

4. Un responsable de la sécurité doit être désigné pour la réunion; il est chargé de la préparation générale et du contrôle des mesures générales de sécurité interne ainsi que de la coordination avec les autres autorités de sécurité concernées. Les dispositions qu'il prend porteront généralement sur:

a) i) les mesures de protection sur le lieu de la réunion pour garantir que celle-ci se déroule sans incident susceptible de compromettre la sécurité des informations classifiées de l'UE qui y seraient utilisées;

ii) le contrôle du personnel ayant accès au lieu de la réunion, aux zones occupées par les délégations et aux salles de conférence, et des matériels qui y sont introduits;

iii) la coordination permanente avec les autorités compétentes de l'État membre d'accueil et avec le Bureau de sécurité du SGC;

b) l'inclusion, dans le dossier de la réunion, d'instructions de sécurité tenant compte des impératifs énoncés dans le présent règlement de sécurité, ainsi que de toute autre consigne de sécurité jugée nécessaire.

Bureau de sécurité du SGC

5. Le Bureau de sécurité du SGC doit jouer un rôle de conseiller en matière de sécurité pour la préparation de la réunion; il doit y être représenté pour aider et conseiller le responsable de la sécurité de la réunion et les délégations, le cas échéant.

6. Chaque délégation à une réunion doit désigner un responsable de la sécurité. Celui-ci est chargé de traiter les questions de sécurité au sein de sa délégation et de rester en liaison avec le responsable de la sécurité de la réunion, ainsi qu'avec le représentant du Bureau de sécurité du SGC, le cas échéant.

MESURES DE SÉCURITÉ

Zones de sécurité

7. Il y a lieu de créer les zones de sécurité suivantes:

   a) une zone de sécurité de catégorie II, comprenant une salle de rédaction, les bureaux et les installations de reproduction du SGC, ainsi que les bureaux des délégations, le cas échéant;

   b) une zone de sécurité de catégorie I, comprenant la salle de conférence et les cabines des interprètes et des ingénieurs du son;

   c) des zones administratives, comprenant les installations destinées à la presse et les secteurs réservés à l'administration, à la restauration et à l'hébergement, ainsi que la zone immédiatement adjacente au centre de presse et au lieu de la réunion.

Laissez-passer

8. Le responsable de la sécurité de la réunion doit établir des badges de type adéquat en fonction des besoins exprimés par les délégations. Le cas échéant, une distinction peut être faite pour l'accès aux différentes zones de sécurité.

9. Les instructions de sécurité relatives à la réunion stipulent que toutes les personnes concernées doivent porter leur badge en permanence et de façon visible dans les locaux de la réunion, afin de permettre au personnel de sécurité d'effectuer les vérifications nécessaires.

10. Outre les participants munis de badges, il y a lieu d'admettre le moins de personnes possible sur le lieu de la réunion. Les délégations nationales souhaitant recevoir des visiteurs pendant la réunion doivent en informer le responsable de la sécurité de la réunion. Les visiteurs se voient remettre un badge spécial; un laissez-passer portant leur nom ainsi que celui de la personne qui les reçoit est établi. Ils doivent être accompagnés en permanence par un garde de sécurité ou par la personne qui les reçoit. Le laissez-passer doit être porté par l'accompagnateur, qui le rend avec le badge de visiteur au personnel de sécurité lorsque le visiteur quitte le lieu de la réunion.

Contrôle des appareils photographiques et des appareils d'enregistrement

11. Aucun appareil photographique ou appareil d'enregistrement ne peut être introduit dans une zone de sécurité de catégorie I, à l'exception du matériel apporté par les photographes et par les ingénieurs du son dûment autorisés par le responsable de la sécurité de la réunion.

Contrôle des porte-documents, ordinateurs portatifs et paquets

12. Les personnes munies d'un laissez-passer leur donnant accès à une zone de sécurité peuvent normalement introduire sans contrôle leurs porte-documents et ordinateurs portatifs (autonomes uniquement). Les délégations peuvent prendre livraison des paquets qui leur sont destinés, après vérification par le responsable de la sécurité de la délégation, ou inspection au moyen d'un matériel spécial, ou après ouverture par le personnel de sécurité. Si le responsable de la sécurité de la réunion le juge nécessaire, des dispositions plus strictes pourront être instaurées pour le contrôle des porte-documents et des paquets.

Sécurité technique

13. Une équipe de sécurité technique peut garantir la sécurité technique de la salle de réunion et assurer également la surveillance électronique en cours de réunion.

Documents des délégations

14. Les délégations sont responsables du transport des documents classifiés de l'UE qu'elles détiennent à destination et au départ des réunions. Elles sont également responsables du contrôle et de la sécurité de ces documents lors de leur utilisation dans les locaux qui leur sont attribués. Le concours de l'État membre d'accueil pourra être demandé pour le transport des documents classifiés à destination ou au départ du lieu de la réunion.

Conservation des documents en lieu sûr

15. Lorsque le SGC, la Commission ou les délégations ne sont pas en mesure de mettre en sûreté leurs documents classifiés selon les normes agréées, ils peuvent confier ces documents, sous enveloppe cachetée et contre récépissés, au responsable de la sécurité de la réunion, à charge pour celui-ci de les mettre à l'abri conformément aux normes agréées.

Vérification des bureaux

16. Le responsable de la sécurité de la réunion doit veiller à ce que les bureaux du SGC et des délégations fassent l'objet d'une vérification après chaque journée de travail, afin de s'assurer que tous les documents classifiés de l'UE ont été mis en lieu sûr; si tel n'est pas le cas, il doit prendre les mesures nécessaires.

Élimination des rebuts classifiés de l'UE

17. Tous les rebuts doivent être considérés comme classifiés de l'UE et le SGC et les délégations se verront remettre des corbeilles à papier ou des sacs pour leur stockage. Avant de quitter les locaux qui leur ont été attribués, le SGC et les délégations doivent porter ces rebuts au responsable de la sécurité de la réunion, qui doit veiller à leur destruction selon les procédures réglementaires.

18. À la fin de la réunion, tous les documents détenus par le SGC ou les délégations et devenus inutiles sont traités comme rebuts. Une fouille approfondie des bureaux du SGC et des délégations doit être effectuée avant la levée des mesures de sécurité prises pour la réunion. Dans la mesure du possible, les documents pour lesquels un reçu a été signé sont détruits comme indiqué à la section VII.

SECTION X

INFRACTIONS À LA SÉCURITÉ ET COMPROMISSION D'INFORMATIONS CLASSIFIÉES DE L'UE

1. L'infraction à la sécurité est un acte ou une omission contraire à une règle de sécurité du Conseil ou nationale et susceptible de mettre en danger ou de compromettre des informations classifiées de l'UE.

2. Il y a compromission, lorsque des informations classifiées de l'UE tombent, totalement ou en partie, aux mains de personnes non autorisées, c'est-à-dire non titulaires de l'habilitation UE appropriée ou n'ayant pas le besoin d'en connaître, ou lorsqu'il est vraisemblable qu'une telle situation se soit produite.

3. La compromission d'informations classifiées de l'UE peut survenir à la suite d'un manque d'attention, d'une négligence ou d'une indiscrétion, ou du fait d'activités de services prenant pour cibles l'UE ou ses États membres et s'intéressant aux informations classifiées et aux activités de l'UE, ou d'organisations subversives.

4. Il importe que toutes les personnes ayant à traiter des informations classifiées de l'UE soient pleinement informées des procédures de sécurité, des dangers de toute conversation indiscrète et des relations qu'elles doivent avoir avec la presse. Elles doivent avoir conscience qu'il est important de rendre compte sans délai de toute infraction à la sécurité qu'elles pourraient remarquer à l'autorité chargée de la sécurité de l'État membre, de l'institution ou de l'organisme dans lequel elles sont employées.

5. Lorsqu'une autorité chargée de la sécurité constate ou est informée que les règles de sécurité ont été enfreintes à l'égard d'informations classifiées de l'UE ou que des matériels classifiés de l'UE sont perdus ou ont disparu, elle doit agir rapidement pour:

   a) établir les faits;

   b) évaluer et réduire au minimum les dommages;

   c) éviter que les faits ne se reproduisent;

   d) informer les autorités compétentes des conséquences de cette infraction.

   À cet égard, les informations suivantes doivent être fournies:

   i) une description des informations concernées, en précisant notamment la classification, la référence, le numéro de l'exemplaire, la date, l'autorité d'origine, l'objet et la portée du document;

   ii) une brève description des circonstances de l'infraction, y compris la date et la période pendant lesquelles l'information a été exposée à une compromission;

   iii) une déclaration indiquant si l'autorité d'origine a été informée.

6. Il est du devoir de toute autorité chargée de la sécurité qui est informée qu'une infraction a pu avoir lieu de le signaler immédiatement, selon la procédure suivante: le bureau d'ordre TRÈS SECRET UE/EU TOP SECRET subordonné porte l'incident à la connaissance du Bureau de sécurité du SGC par la voie de son bureau d'ordre TRÈS SECRET UE/EU TOP SECRET central; dans le cas d'une compromission d'une information classifiée de l'UE survenant dans la juridiction d'un État membre, l'incident doit être porté, conformément aux dispositions du point 5, à la connaissance du Bureau de sécurité du SGC par l'intermédiaire de l'ANS responsable.

7. En ce qui concerne les informations RESTREINT UE, des rapports ne sont établis que lorsque les cas présentent des caractéristiques inhabituelles.

8. Dès qu'il est informé d'une infraction, le Secrétaire général/Haut représentant:

   a) la notifie à l'autorité d'origine qui a fourni les informations classifiées en question;

   b) invite l'autorité de sécurité compétente à ouvrir une enquête;

   c) coordonne les enquêtes si plusieurs autorités de sécurité sont concernées;

d) se fait remettre un rapport sur les circonstances de l'infraction, la date ou la période à laquelle elle a pu se produire, la date et le lieu de sa découverte et une description détaillée du contenu et de la classification des documents concernés. Le préjudice causé aux intérêts de l'UE ou de l'un ou de plusieurs de ses États membres et les mesures prises pour éviter toute répétition des faits doivent également être indiqués.

9. L'autorité d'origine informe les destinataires et donne les instructions appropriées.

10. Toute personne dont la responsabilité est engagée dans une compromission d'informations classifiées de l'UE est passible de sanctions disciplinaires conformément à la réglementation applicable et sans préjudice de poursuites en justice.

SECTION XI

PROTECTION DES INFORMATIONS TRAITÉES DANS DES SYSTÈMES DES TECHNOLOGIES DE L'INFORMATION ET DANS DES SYSTÈMES DES COMMUNICATION

Sommaire

Chapitre I

Introduction

GÉNÉRALITÉS

1. La doctrine de sécurité et les exigences en la matière qui sont définies dans la présente section s'appliquent à tous les systèmes et réseaux de communication et d'information (ci-après dénommés «SYSTÈMES») qui traitent des informations CONFIDENTIEL UE ou d'une classification supérieure.

2. Les SYSTÈMES qui traitent des informations RESTREINT UE nécessitent aussi l'application de mesures de sécurité destinées à protéger la confidentialité de ces informations. Tous les SYSTÈMES nécessitent des mesures de sécurité permettant de protéger l'intégrité et la disponibilité de ces systèmes et des informations qu'ils contiennent. Les mesures de sécurité à appliquer à ces systèmes sont arrêtées par l'autorité d'homologation de sécurité (SAA) compétente; elles sont proportionnelles au risque estimé et compatibles avec la doctrine énoncée dans le présent règlement de sécurité.

3. La protection des systèmes de détection comportant des SYSTÈMES TI est déterminée et énoncée dans le cadre général des systèmes auxquels ils appartiennent, en appliquant, dans toute la mesure du possible, les dispositions pertinentes de la présente section.

VULNÉRABILITÉ DES SYSTÈMES ET MENACES ÉVENTUELLES

4. D'une manière générale, une menace peut être définie comme une possibilité de compromission accidentelle ou délibérée de la sécurité. Dans le cas des SYSTÈMES, cette compromission se traduit par la perte de l'une ou de plusieurs des qualités que sont la confidentialité, l'intégrité et la disponibilité. La vulnérabilité peut être définie comme une faiblesse ou un manque de contrôles qui faciliterait ou qui permettrait la concrétisation d'une menace pesant sur un bien ou un objectif spécifique. La vulnérabilité peut résulter d'une omission ou être liée à un contrôle trop faible, incomplet ou inégal. Elle peut se situer sur le plan de la technique, des procédures ou de l'exploitation.

5. Les informations classifiées ou non de l'UE traitées dans des SYSTÈMES sous une forme condensée permettant de les retrouver, de les communiquer et de les utiliser rapidement sont exposées à de nombreux risques. Il peut s'agir de l'accès à ces informations par des utilisateurs non autorisés ou, au contraire, de l'impossibilité pour des utilisateurs autorisés d'y avoir accès. Il existe aussi des risques de divulgation, d'altération, de modification ou d'effacement non autorisés de ces informations. De plus, le matériel, complexe et parfois fragile, est coûteux et souvent difficile à réparer ou à remplacer rapidement. Ces systèmes constituent ainsi des cibles toutes désignées pour des opérations de collecte de renseignements et pour des actes de sabotage, surtout si les mesures de sécurité paraissent inefficaces.

MESURES DE SÉCURITÉ

6. Les mesures de sécurité énoncées dans la présente section ont pour principal objectif d'assurer la protection contre la divulgation non autorisée d'informations (la perte de confidentialité) ainsi que contre la perte d'intégrité et de disponibilité des informations. Pour assurer une protection convenable aux SYSTÈMES qui traitent des informations classifiées de l'UE, il est nécessaire de spécifier les normes appropriées de protection classique, de même que les procédures et techniques adéquates de sécurité conçues spécialement pour chaque SYSTÈME.

7. Un ensemble équilibré de mesures de sécurité doit être élaboré et mis en œuvre, en vue de créer un environnement protégé dans lequel un SYSTÈME fonctionne. Les domaines d'application de ces mesures concernent les éléments physiques, le personnel, les procédures non techniques et les procédures d'exploitation des ordinateurs et des communications.

8. On doit prévoir pour les ordinateurs des mesures de sécurité (dispositifs de sécurité matériels et logiciels) qui permettent d'appliquer le principe du besoin d'en connaître et d'éviter ou de détecter la divulgation non autorisée d'informations. La confiance que l'on peut accorder aux mesures de sécurité applicables aux ordinateurs est déterminée au cours du processus de définition des exigences de sécurité. Le processus d'homologation permet d'établir qu'il existe un niveau d'assurance suffisant pour justifier cette confiance dans ces mesures.

ÉNONCÉ DES IMPÉRATIFS DE SÉCURITÉ PROPRES À UN SYSTÈME (SSRS)

9. Pour tous les SYSTÈMES qui traitent des informations CONFIDENTIEL UE ou d'une classification supérieure, un énoncé des impératifs de sécurité propres à un SYSTÈME (SSRS) doit être établi par l'autorité d'exploitation du système TI (ITSOA), le cas échéant avec la contribution et l'assistance des responsables de projet et de l'autorité INFOSEC, et approuvé par la SAA. Un SSRS doit également être établi lorsque la disponibilité et l'intégrité des informations RESTREINT UE ou des informations non classifiées est jugée essentielle par la SAA.

10. Le SSRS est élaboré le plus tôt possible au cours de la conception d'un projet et doit être développé et amélioré au fur et à mesure que celui-ci prend corps. Il joue différents rôles aux différents stades du cycle de vie du projet et du SYSTÈME.

11. Le SSRS constitue l'accord liant l'autorité d'exploitation du système TI et la SAA, en fonction duquel le SYSTÈME doit être homologué.

12. Le SSRS est un exposé complet et explicite des principes de sécurité à observer et de tous les aspects des exigences de sécurité à satisfaire. Il se fonde sur la doctrine de sécurité du Conseil et sur une analyse des risques, ou est déterminé par des paramètres tels que les conditions d'exploitation, le niveau minimum d'habilitation du personnel, le niveau maximum de classification des informations traitées, le mode d'exploitation de sécurité ou les besoins des utilisateurs. Le SSRS fait partie intégrante de la documentation relative au projet qui est soumise aux autorités compétentes pour approbation sur le plan technique, budgétaire et de la sécurité. Il constitue dans sa version définitive un énoncé complet des critères auxquels doit répondre le SYSTÈME pour être sûr.

MODES D'EXPLOITATION DE SÉCURITÉ

13. Tous les SYSTÈMES qui traitent des informations CONFIDENTIEL UE ou d'une classification supérieure font l'objet d'une homologation qui autorise leur exploitation selon un ou, si les besoins le justifient sur différentes périodes, plusieurs des modes d'exploitation de sécurité ci-après, ou leur équivalent national:

a) mode exclusif;

b) mode dominant, et

c) mode multiniveau.

Chapitre II

Définitions

TIMBRES COMPLÉMENTAIRES

14. Les timbres complémentaires tels que CRYPTO ou toute autre désignation exigeant un traitement spécial reconnue par l'UE sont utilisés lorsqu'un document doit faire l'objet d'une diffusion limitée et d'un traitement spécial qui s'ajoute à celui qu'exige la classification de sécurité.

15. Par MODE D'EXPLOITATION DE SÉCURITÉ «EXCLUSIF», on entend un mode d'exploitation selon lequel TOUTES les personnes ayant accès au SYSTÈME sont habilitées au plus haut niveau de classification des informations traitées au sein du SYSTÈME, et ont un besoin commun d'en connaître pour TOUTES les informations traitées au sein du SYSTÈME.

Notes:

(1) Avec le besoin commun d'en connaître, il n'est pas absolument nécessaire que des dispositifs de sécurité informatique assurent la séparation des informations au sein du SYSTÈME.

(2) Les autres dispositifs de sécurité (applicables, par exemple, aux aspects physiques, aux agents et aux procédures) doivent répondre aux exigences fixées pour le plus haut niveau de classification et pour toute désignation de catégorie des informations traitées au sein du SYSTÈME.

16. Par MODE D'EXPLOITATION DE SÉCURITÉ «DOMINANT», on entend un mode d'exploitation selon lequel les personnes qui ont accès au SYSTÈME sont TOUTES habilitées au plus haut niveau de classification des informations traitées au sein du SYSTÈME, mais n'ont PAS TOUTES un besoin commun d'en connaître pour les informations traitées au sein du SYSTÈME.

Notes:

(1) Le fait que les personnes en question n'ont pas un besoin commun d'en connaître rend nécessaires des dispositifs de sécurité informatique assurant un accès sélectif aux informations présentes dans le SYSTÈME, ainsi que la séparation de ces informations.

(2) Les autres dispositifs de sécurité (applicables, par exemple, aux aspects physiques, aux agents et aux procédures) doivent répondre aux exigences fixées pour le plus haut niveau de classification et pour toute désignation de catégorie des informations traitées au sein du SYSTÈME.

(3) Toutes les informations traitées ou utilisables par un SYSTÈME fonctionnant selon ce mode d'exploitation, de même que toute sortie générée, doivent être protégées comme étant potentiellement de la catégorie et du plus haut degré de classification des données traitées, jusqu'à preuve du contraire, à moins qu'il n'existe une fonction d'étiquetage suffisamment fiable.

17. Par MODE D'EXPLOITATION DE SÉCURITÉ «MULTINIVEAU», on entend un mode d'exploitation dans lequel les personnes ayant accès au SYSTÈME ne sont PAS TOUTES habilitées au plus haut niveau de classification des informations traitées au sein du SYSTÈME, et n'ont PAS TOUTES un besoin commun d'en connaître pour les informations traitées au sein du SYSTÈME.

Notes:

(1) Ce mode d'exploitation permet, simultanément, le traitement d'informations de différents niveaux de classification et de différentes catégories.

(2) Le fait que les personnes en question ne soient pas toutes habilitées au plus haut niveau et qu'elles n'ont pas un besoin commun d'en connaître rend nécessaires des dispositifs de sécurité informatique assurant un accès sélectif aux informations présentes dans le SYSTÈME, ainsi que la séparation de ces informations.

18. Par INFOSEC, on entend l'application de mesures de sécurité destinées à protéger les informations traitées, stockées ou transmises par des systèmes de communication, d'information et autres systèmes électroniques, contre les atteintes à la confidentialité, à l'intégrité ou à la disponibilité de ces informations, que celles-ci soient accidentelles ou intentionnelles, ainsi qu'à empêcher les atteintes à l'intégrité et à la disponibilité des systèmes eux-mêmes. Les mesures INFOSEC recouvrent la sécurité des ordinateurs, des transmissions, des émissions et la sécurité cryptographique, ainsi que la détection des menaces auxquelles sont exposés les informations et les SYSTÈMES, la collecte d'informations à leur sujet et leur prévention.

19. Par SÉCURITÉ DES ORDINATEURS (COMPUSEC), on entend la mise en place, sur un système informatique, de dispositifs de sécurité matériels, microprogrammés, et logiciels, afin de le protéger contre — ou d'empêcher — les divulgations, manipulations, modifications ou suppressions non autorisées d'informations ou la privation d'accès.

20. Par PRODUIT DE SÉCURITÉ INFORMATIQUE, on entend un élément général de sécurité informatique destiné à être incorporé à un système TI afin d'améliorer ou d'assurer la confidentialité, l'intégrité ou la disponibilité des informations traitées.

21. Par SÉCURITÉ DES COMMUNICATIONS (COMSEC), on entend l'application aux télécommunications de mesures de sécurité ayant pour but d'empêcher des personnes non autorisées d'obtenir des informations utiles en entrant en possession et en étudiant des messages communiqués, ou d'assurer l'authenticité de ces messages.

Note:

Ces mesures visent non seulement la sécurité des moyens de chiffrement, des transmissions et des émissions, mais aussi la sécurité relative aux procédures, aux éléments physiques, au personnel et la sécurité des documents ainsi que la sécurité informatique.

22. Par ÉVALUATION, on entend l'examen technique détaillé, par une autorité compétente, des aspects d'un SYSTÈME, d'un moyen de chiffrement ou d'un produit de sécurité informatique qui ont un rapport avec sa sécurité.

Notes:

(1) L'évaluation porte sur la présence de la fonctionnalité de sécurité requise, sur l'absence d'effets secondaires indésirables découlant de cette fonctionnalité et sur le caractère inaltérable de celle-ci.

(2) L'évaluation détermine dans quelle mesure sont satisfaits les impératifs de sécurité d'un SYSTÈME, ou justifiées les prétentions d'un produit de sécurité informatique, et détermine le niveau d'assurance du SYSTÈME ou du moyen de chiffrement, ou de la fonction de confiance du produit de sécurité informatique.

23. Par CERTIFICATION, on entend la délivrance d'un document officiel fondé sur un examen indépendant de la conduite et des résultats d'une évaluation et indiquant dans quelle mesure un SYSTÈME répond à l'exigence de sécurité, ou un produit de sécurité informatique possède bien dans ce domaine les caractéristiques préalablement établies.

24. Par HOMOLOGATION, on entend l'agrément d'un SYSTÈME autorisant son emploi pour traiter des informations classifiées de l'UE dans son environnement opérationnel.

Note:

Cette homologation doit se faire après l'application de toutes les procédures de sécurité appropriées et l'obtention d'un niveau de protection suffisant pour les éléments du système. L'homologation doit normalement s'appuyer sur le SSRS, notamment sur les éléments suivants:

a) une définition de l'objectif de l'homologation du système, indiquant en particulier les niveaux de classification des informations à traiter et le ou les modes d'exploitation de sécurité proposés pour le système ou le réseau;

b) une analyse des risques, identifiant les menaces et les vulnérabilités, ainsi que les mesures nécessaires pour les prévenir;

c) les procédures d'exploitation de sécurité (SecOP) avec une description détaillée des opérations prévues (par exemple, les modes et les services à fournir) et notamment des dispositifs de sécurité du SYSTÈME qui serviront de base à l'homologation;

d) le plan de mise en place et de maintenance des dispositifs de sécurité;

e) le plan prévoyant les tests, l'évaluation et la certification visant à assurer la sécurité initiale et ultérieure du système ou du réseau, et

f) la certification, s'il y a lieu, ainsi que les autres éléments d'homologation.

25. Par SYSTÈME TI, on entend l'ensemble des matériels, méthodes et procédures et, le cas échéant, des personnes, organisé de façon à remplir des fonctions de traitement de l'information.

Notes:

(1) Il s'agit d'un ensemble des moyens organisés pour le traitement d'informations à l'intérieur du système.

(2) Ces systèmes peuvent être utilisés pour des fonctions de consultation, de commande, de surveillance et de communication, de même que pour des applications scientifiques ou administratives, dont le traitement de texte.

(3) Un système est généralement défini comme étant un ensemble d'éléments se trouvant sous le contrôle d'une seule autorité d'exploitation du système TI (ITSOA).

(4) Un système TI peut contenir des sous-systèmes dont certains sont eux-mêmes des systèmes TI.

26. Les DISPOSITIFS DE SÉCURITÉ D'UN SYSTÈME TI comprennent toutes les fonctions, caractéristiques et dispositifs matériels, microprogrammés et logiciels; les procédures d'exploitation et d'établissement des responsabilités et les contrôles de l'accès, la zone TI, la zone des terminaux ou postes de travail distants, ainsi que les règles de gestion, les dispositifs et structures physiques, et les mesures de contrôle du personnel et des communications nécessaires pour assurer un niveau acceptable de protection aux informations classifiées qui doivent être traitées dans un système TI.

27. Par RÉSEAU TI, on entend un ensemble, géographiquement dispersé, constitué de systèmes TI interconnectés pour échanger des données, et comprenant les divers éléments des systèmes TI interconnectés et leurs interfaces avec les réseaux de données ou de communications qui les complètent.

Notes:

(1) Un réseau TI peut faire appel aux services d'un ou de plusieurs réseaux de communication pour échanger des données; plusieurs réseaux TI peuvent faire appel aux services d'un réseau de communication commun.

(2) Un réseau TI est qualifié de «local» s'il relie entre eux plusieurs ordinateurs se trouvant sur le même site.

28. Les DISPOSITIFS DE SÉCURITÉ D'UN RÉSEAU TI comprennent les dispositifs de sécurité de chaque système TI faisant partie du réseau, mais aussi les composantes et dispositifs supplémentaires associés au réseau même et nécessaires pour assurer un niveau acceptable de protection aux informations classifiées (par exemple, les communications sur le réseau, les mécanismes et procédures d'étiquetage et d'identification de sécurité, les contrôles d'accès, les programmes et les fichiers de suivi).

29. Par ZONE TI, on entend une zone qui contient un ou plusieurs ordinateurs, avec leurs unités de stockage et leurs périphériques locaux, leurs unités de commande et le matériel de réseau et de communications qui leur est réservé.

Note:

Ne fait pas partie de cette zone, toute zone séparée où se trouvent des terminaux, postes de travail ou périphériques distants, même si ces dispositifs sont connectés au matériel se trouvant dans la zone TI.

30. Par ZONE DE TERMINAUX OU POSTES DE TRAVAIL DISTANTS, on entend une zone séparée d'une zone TI, contenant du matériel informatique, ses périphériques, terminaux ou postes de travail locaux et le matériel de communications associé.

31. Par contre-mesures TEMPEST, on entend des mesures de sécurité destinées à protéger le matériel et les infrastructures de communication contre la compromission d'informations classifiées par l'émission non intentionnelle de rayonnements électromagnétiques.

Chapitre III

Responsabilités en matière de sécurité

GÉNÉRALITÉS

32. Les responsabilités du Comité de sécurité, définies à la section I, point 4, incluent les questions INFOSEC. Le Comité de sécurité organise ses activités de manière à être en mesure de fournir des conseils de spécialistes concernant les questions précitées.

33. En cas de problème ayant trait à la sécurité (incidents, infractions, etc.), l'autorité nationale compétente et/ou le Bureau de sécurité du SGC prennent immédiatement des mesures. Tout problème doit être soumis au Bureau de sécurité du SGC.

34. Le Secrétaire général/Haut représentant ou, le cas échéant, le chef d'un organisme décentralisé de l'UE, crée un Bureau INFOSEC chargé de fournir des lignes directrices à l'autorité de sécurité concernant la mise en œuvre et le contrôle des dispositifs spéciaux de sécurité intégrés aux SYSTÈMES.

AUTORITÉ D'HOMOLOGATION DE SÉCURITÉ (SAA)

35. La SAA est:

— soit une ANS,

— soit l'autorité désignée par le Secrétaire général/Haut représentant,

— soit l'autorité de sécurité d'un organisme décentralisé de l'UE,

— soit des représentants délégués ou nommés par eux, selon le SYSTÈME à homologuer.

36. La SAA est responsable de la conformité des SYSTÈMES avec la doctrine de sécurité du Conseil. Elle est chargée de prononcer l'homologation d'un SYSTÈME pour traiter des informations classifiées de l'UE à un niveau de classification déterminé dans son environnement d'exploitation. En ce qui concerne le SGC et, le cas échéant, les organismes décentralisés de l'UE, la SAA est responsable de la sécurité au nom du Secrétaire général/Haut représentant ou des chefs des organismes décentralisés.

Tous les SYSTÈMES exploités dans les locaux du SGC relèvent de la juridiction de la SAA du SGC. Les SYSTÈMES et les éléments de SYSTÈMES qui sont exploités dans un État membre restent sous la juridiction de cet État membre. Lorsque différents éléments d'un même SYSTÈME passent sous la juridiction de la SAA du SGC et d'autres SAA, toutes les parties concernées désignent un comité conjoint d'homologation, la coordination étant assurée par la SAA du SGC.

AUTORITÉ CHARGÉE DE LA SÉCURITÉ INFORMATIQUE (INFOSEC)

37. L'autorité INFOSEC est responsable des activités du Bureau INFOSEC. En ce qui concerne le SGC et, le cas échéant, les organismes décentralisés de l'UE, l'autorité INFOSEC a pour responsabilités:

— de conseiller et d'assister la SAA sur le plan technique,

— de contribuer à l'élaboration du SSRS,

— d'examiner le SSRS pour assurer sa compatibilité avec le présent règlement de sécurité ainsi que les politiques INFOSEC et les documents relatifs à l'architecture,

— de participer aux commissions/comités d'homologation, le cas échéant, et de fournir à la SAA des recommandations INFOSEC concernant l'homologation,

— d'apporter un soutien aux activités d'éducation et de formation INFOSEC,

— de fournir des conseils techniques dans le cadre des enquêtes sur des incidents ayant trait à l'INFOSEC,

— élaborer des lignes directrices techniques pour faire en sorte que seuls des logiciels autorisés soient utilisés.

AUTORITÉ D'EXPLOITATION DU SYSTÈME TI (ITSOA)

38. L'autorité INFOSEC délègue le plus rapidement possible à ITSOA la responsabilité de la mise en œuvre des contrôles et du fonctionnement des dispositifs de sécurité spéciaux du SYSTÈME. Cette responsabilité est exercée pendant tout le cycle de vie du SYSTÈME, de la conception du projet à sa liquidation finale.

39. L'ITSOA est responsable de tous les dispositifs de sécurité conçus comme partie intégrante du SYSTÈME dans son ensemble. Elle est notamment chargée de l'élaboration des SecOP et décide des normes et pratiques de sécurité auxquelles doit se conformer le fournisseur du SYSTÈME.

40. L'ITSOA peut déléguer une partie de ses responsabilités, en tant que de besoin, par exemple aux responsables INFOSEC chargés respectivement du système et du site. Les différentes fonctions INFOSEC peuvent être assumées par une seule personne.

UTILISATEURS

41. Tous les utilisateurs ont pour responsabilité de veiller à ce que leurs actes ne portent pas préjudice à la sécurité du SYSTÈME qu'ils utilisent.

FORMATION INFOSEC

42. Au sein du SGC, des organismes décentralisés de l'UE ou des services officiels des États membres, une instruction et une formation doivent être assurées en matière d'INFOSEC, à divers niveaux et pour les différents agents, en fonction des besoins.

Chapitre IV

Mesures de sécurité non techniques

MESURES DE SÉCURITÉ CONCERNANT LE PERSONNEL

43. Les utilisateurs du SYSTÈME doivent être titulaires d'une habilitation correspondant à la classification et au contenu des informations traitées dans leur SYSTÈME particulier, et doivent avoir besoin d'en connaître. L'accès à certains équipements ou informations spécifiques à la sécurité des SYSTÈMES nécessite une habilitation particulière délivrée selon les procédures du Conseil en vigueur.

44. La SAA doit désigner tous les postes sensibles et définir le niveau d'habilitation et de surveillance nécessaire pour tous les agents travaillant à ces postes.

45. Les SYSTÈMES doivent être spécifiés et conçus d'une manière qui facilite la répartition des tâches et responsabilités entre les membres du personnel informatique de façon qu'aucune personne n'ait la connaissance ni le contrôle complet des points clés du système. L'objectif recherché est que personne ne puisse opérer de modifications ou d'actes malveillants sur le système ou réseau sans la complicité d'une ou de plusieurs autres personnes.

SÉCURITÉ PHYSIQUE

46. Les zones TI et les zones de terminaux ou postes de travail distants (telles que définies aux points 29 et 30) dans lesquelles des informations classifiées CONFIDENTIEL UE ou d'une classification supérieure sont traitées au moyen de technologies de l'information, ou dans lesquelles l'accès à de telles informations est possible, sont désignées, selon le cas, comme zones de sécurité UE de catégorie I ou II, ou leur équivalent national.

47. Un employé autorisé ne doit jamais se trouver seul dans une zone TI ou dans une zone de terminaux ou postes de travail distants où la sécurité du SYSTÈME peut être modifiée.

CONTRÔLE DES ACCÈS À UN SYSTÈME

48. Toutes les informations et tous les matériels qui contrôlent l'accès à un SYSTÈME sont protégés selon des dispositions correspondant à la classification la plus élevée et à la catégorie d'informations auxquelles ce système peut donner accès.

49. Lorsqu'ils ne sont plus utilisés à cette fin, les informations et les matériels de contrôle des accès doivent être détruits conformément aux points 61 à 63.

Chapitre V

Mesures de sécurité techniques

SÉCURITÉ DES INFORMATIONS

50. Il incombe à l'autorité d'origine des informations de recenser et de classifier tous les documents porteurs d'informations, qu'il s'agisse de sorties sous forme de copie papier ou de supports informatiques. Sur chaque page d'une copie papier doit être apposé, en haut et en bas, le timbre indiquant la classification. Les sorties, qu'elles prennent la forme de copies papier ou de supports informatiques, doivent recevoir la classification la plus élevée des informations utilisées pour leur production. Le mode d'exploitation de sécurité d'un SYSTÈME peut aussi avoir une influence sur la classification des sorties de ce système.

51. Il incombe à un organisme et à ceux qui y détiennent des informations d'examiner les problèmes liés au cumul d'éléments d'information discrets et aux recoupements qui peuvent être faits par leur mise en corrélation, pour déterminer si, une fois réunis, ces éléments n'exigent pas une classification plus élevée.

52. Le fait que les informations puissent être représentées sous forme codée abrégée, codée pour transmission ou toute autre forme binaire ne leur assure aucune protection et ne doit donc pas entrer en ligne de compte pour la détermination de leur classification.

53. Lorsque des informations sont transférées d'un SYSTÈME à un autre, elles doivent être protégées au cours du transfert et dans le SYSTÈME récepteur d'une manière adaptée à la classification et à la catégorie initiales des informations.

54. Tous les supports informatiques doivent être traités conformément à la classification la plus élevée des informations stockées ou du marquage et doivent être protégés en permanence de manière appropriée.

55. Les supports informatiques réutilisables ayant servi à enregistrer des informations classifiées de l'UE conservent le niveau de classification le plus élevé attribué aux données pour lesquelles ils ont été utilisés, jusqu'à ce que ces informations aient été déclassées ou déclassifiées comme il convient et le support reclassifié en conséquence, déclassifié ou détruit selon une procédure du SGC ou nationale agréée (voir points 61 à 63).

CONTRÔLE ET COMPTABILISATION DES INFORMATIONS

56. Les accès à des informations SECRET UE ou d'un niveau de classification supérieur doivent être consignés automatiquement (fichiers de suivi) ou manuellement dans un registre. Ces registres sont conservés conformément aux dispositions du présent règlement de sécurité.

57. Les sorties classifiées qui sont détenues à l'intérieur de la zone TI peuvent être considérées comme un même ensemble d'informations classifiées et n'ont pas à être enregistrées, à condition d'être identifiées, de porter la mention de leur niveau de classification et d'être contrôlées de façon appropriée.

58. Lorsque des données sortant d'un SYSTÈME qui traite des informations classifiées de l'UE sont transmises à un terminal ou poste de travail distant à partir d'une zone TI, des procédures agréées par la SAA doivent être établies en vue de contrôler les données ainsi disséminées. Pour les informations SECRET UE et au-delà, ces procédures comprennent des instructions particulières de comptabilisation des informations.

MANIPULATION ET CONTRÔLE DES SUPPORTS AMOVIBLES

59. Tous les supports informatiques amovibles d'une classification égale ou supérieure à CONFIDENTIEL UE sont traités comme des matériels classifiés et obéissent aux prescriptions générales y afférentes. Les moyens utilisés pour les identifier et indiquer leur classification doivent être adaptés à la nature physique de chacun, dans un souci de lisibilité.

60. Il incombe aux utilisateurs de s'assurer que les informations classifiées de l'UE sont enregistrées sur des supports portant le marquage de classification approprié et bénéficient de la protection requise. Des procédures doivent être établies afin que, pour tous les niveaux d'informations de l'UE, la mise en mémoire sur des supports informatiques se fasse conformément au présent règlement de sécurité.

DÉCLASSIFICATION ET DESTRUCTION DES SUPPORTS INFORMATIQUES

61. Les supports informatiques ayant servi à enregistrer des informations classifiées de l'UE peuvent être déclassés ou déclassifiés, à condition qu'une procédure du SGC ou nationale agréée soit appliquée.

62. Les supports ayant contenu des informations TRÈS SECRET UE/EU TOP SECRET ou d'une catégorie spéciale ne doivent pas être déclassifiés ni réutilisés.

63. Les supports qui ne peuvent être ni déclassifiés ni réutilisés sont détruits selon une procédure du SGC ou nationale agréée.

SÉCURITÉ DES COMMUNICATIONS

64. Lorsque des informations classifiées de l'UE sont transmises par voie électromagnétique, des mesures particulières sont mises en œuvre pour protéger la confidentialité, l'intégrité et la disponibilité des informations transmises. La SAA détermine les exigences à satisfaire pour protéger les transmissions d'une éventuelle détection et interception. Les informations transmises au moyen d'un système de communication sont protégées sur la base des exigences nécessaires pour assurer leur confidentialité, leur intégrité et leur disponibilité.

65. Lorsqu'il est nécessaire de recourir à des méthodes cryptographiques pour protéger la confidentialité, l'intégrité et la disponibilité des informations, ces méthodes ou les produits qui leur sont associés doivent être spécialement agréés à cet effet par la SAA.

66. Pendant la transmission, la confidentialité des informations SECRET UE ou d'un niveau de classification supérieur doit être protégée par des méthodes ou des produits cryptographiques agréés par le Conseil sur recommandation du Comité de sécurité du Conseil. Pendant la transmission, la confidentialité des informations CONFIDENTIEL UE ou RESTREINT UE doit être protégée par des méthodes ou des produits cryptographiques agréés soit par le Secrétaire général/Haut représentant sur recommandation du Comité de sécurité du Conseil, soit par un État membre.

67. Les règles détaillées applicables à la transmission d'informations classifiées de l'UE doivent figurer dans des instructions de sécurité spécifiques approuvées par le Conseil sur recommandation du Comité de sécurité du Conseil.

68. Dans des circonstances exceptionnelles, les informations RESTREINT UE, CONFIDENTIEL UE et SECRET UE peuvent êtres transmises en clair, à condition que chacune de ces transmissions fasse l'objet d'une autorisation expresse. Ces conditions exceptionnelles sont les suivantes:

    a) en cas de crise, de conflit ou de guerre imminents ou pendant l'un de ces événements, et

    b) en cas d'urgence extrême et en l'absence de moyens de chiffrement, lorsqu'on estime que les informations transmises ne peuvent pas être exploitées dans les délais permettant d'influer sur le déroulement des opérations en cours.

69. Un SYSTÈME doit être capable de refuser catégoriquement l'accès aux informations classifiées de l'UE au niveau de l'un ou de l'ensemble de ses postes de travail ou terminaux distants, le cas échéant par une déconnexion physique ou par des dispositifs logiciels spéciaux approuvés par la SAA.

MESURES DE SÉCURITÉ CONCERNANT L'INSTALLATION ET LE RAYONNEMENT

70. Les spécifications établies pour l'installation initiale d'un SYSTÈME et pour toute modification importante ultérieure précisent que les travaux doivent être effectués par des installateurs ayant l'habilitation de sécurité nécessaire, sous la surveillance permanente d'un personnel technique compétent habilité à avoir accès à des informations de l'UE d'un niveau de classification équivalant à la classification la plus élevée des informations que le SYSTÈME est appelé à conserver et à traiter.

71. Tout le matériel doit être installé conformément aux dispositions de sécurité du Conseil en vigueur.

72. Les SYSTÈMES qui traitent des informations CONFIDENTIEL UE ou d'une classification supérieure sont protégés de telle manière que leur sécurité ne puisse être menacée par des rayonnements compromettants, dont l'étude et la prévention sont désignés par le terme «TEMPEST».

73. Les contre-mesures TEMPEST applicables aux installations du SGC et des organismes décentralisés de l'UE sont étudiées et approuvées par une autorité d'homologation TEMPEST désignée par l'autorité de sécurité du SGC. Pour les installations nationales qui servent à traiter des informations classifiées de l'UE, l'autorité d'homologation est l'instance d'homologation TEMPEST nationale officielle.

Chapitre VI

Sécurité pendant le traitement

PROCÉDURES D'EXPLOITATION DE SÉCURITÉ

74. Les SecOP définissent les principes à adopter en matière de sécurité, les procédures d'exploitation à suivre et les responsabilités du personnel. Les SecOP sont élaborées sous la responsabilité de l'ITSOA.

PROTECTION ET GESTION DE LA CONFIGURATION DES LOGICIELS

75. Le niveau de protection des programmes d'application est déterminé en fonction d'une évaluation de la classification de sécurité du programme lui-même, plutôt que de celle des informations qu'il doit traiter. Les versions des logiciels utilisées doivent être vérifiées à intervalles réguliers de façon à s'assurer de leur intégrité et de leur bon fonctionnement.

76. Les nouvelles versions ou versions modifiées des logiciels ne seront utilisées pour le traitement d'informations classifiées de l'UE qu'après avoir été vérifiées par l'ITSOA.

DÉTECTION DE LA PRÉSENCE DE LOGICIELS MALVEILLANTS OU DE VIRUS INFORMATIQUES

77. La détection de la présence de logiciels malveillants ou de virus informatiques se fait périodiquement en observant les exigences de la SAA.

78. Tout support informatique pénétrant dans le SGC ou dans un organisme décentralisé de l'UE ou dans les services des États membres doit être vérifié avant son introduction dans un SYSTÈME afin d'y détecter la présence éventuelle d'un logiciel malveillant ou d'un virus informatique.

MAINTENANCE

79. Les contrats et procédures en vue de la maintenance périodique et sur demande des SYSTÈMES pour lesquels un SSRS a été établi doivent préciser les exigences et les dispositions applicables au personnel et au matériel de maintenance qui doivent pénétrer dans une zone TI.

80. Les exigences et les procédures doivent être clairement énoncées respectivement dans le SSRS et dans les SecOP. Les opérations de maintenance incombant au contractant et nécessitant des procédures de télédiagnostic ne doivent être autorisées que dans des cas exceptionnels, sous contrôle rigoureux, et avec l'accord de la SAA.

Chapitre VII

Acquisition

81. Les produits de sécurité à utiliser avec le SYSTÈME à acquérir doivent être soit des produits évalués et certifiés, soit des produits en cours d'évaluation et de certification par un organisme d'évaluation ou de certification approprié, selon des critères internationalement reconnus (comme les Critères communs d'évaluation de la sécurité des technologies de l'information, cf. norme ISO 15408).

82. Pour décider si le matériel, notamment les supports de stockage informatique, doit être loué plutôt qu'acheté, on doit tenir compte du fait que ce matériel, une fois utilisé pour le traitement d'informations classifiées de l'UE, ne peut plus quitter les locaux qui lui assurent la protection voulue sans avoir été préalablement déclassifié avec l'approbation de la SAA, approbation qui ne peut pas toujours être donnée.

HOMOLOGATION

83. Avant de traiter des informations classifiées de l'UE, tous les SYSTÈMES pour lesquels un SSRS doit être établi doivent être homologués par la SAA, sur la base des informations contenues dans le SSRS, dans les SecOP et dans tout autre document pertinent. Les sous-systèmes et les terminaux ou postes de travail distants doivent être homologués au même titre que les SYSTÈMES auxquels ils sont raccordés. Lorsqu'un SYSTÈME dessert à la fois le Conseil et d'autres organisations, le SGC et les autorités de sécurité concernées doivent s'accorder sur la question de l'homologation.

84. La procédure d'homologation peut se dérouler conformément à une stratégie d'homologation adaptée au SYSTÈME particulier et définie par la SAA.

ÉVALUATION ET CERTIFICATION

85. Avant qu'un SYSTÈME ne puisse être homologué, il faut, dans certains cas, que les dispositifs de sécurité des matériels, des microprogrammes et des logiciels aient fait l'objet d'une évaluation et d'une certification qui attestent la capacité du SYSTÈME à protéger des informations au niveau de classification voulu.

86. Les exigences en matière d'évaluation et de certification doivent être prévues dans la planification du système et clairement énoncées dans le SSRS.

87. L'évaluation et la certification sont effectuées conformément aux directives approuvées, par des équipes d'agents possédant les compétences techniques nécessaires, titulaires de l'habilitation appropriée et agissant pour le compte de l'ITSOA.

88. Les équipes peuvent être fournies par l'autorité d'évaluation ou de certification d'un État membre désigné ou par ses représentants désignés, par exemple un contractant compétent et habilité.

89. L'évaluation et la certification peuvent être moins poussées (c'est-à-dire ne porter que sur l'intégration, par exemple) lorsque les SYSTÈMES sont fondés sur des produits de sécurité informatique existants évalués et certifiés au niveau national.

CONTRÔLE SYSTÉMATIQUE DES DISPOSITIFS DE SÉCURITÉ POUR LA PROROGATION DE L'HOMOLOGATION

90. L'ITSOA établit des procédures de contrôle systématique garantissant que tous les dispositifs de sécurité du SYSTÈME sont toujours valables.

91. Le SSRS doit clairement recenser et énoncer les types de modifications qui donneraient lieu à une nouvelle homologation ou qui nécessitent une autorisation préalable de l'autorité d'homologation de sécurité. Pour assurer le bon fonctionnement des dispositifs de sécurité, l'ITSOA fait procéder à une vérification après toute modification, réparation ou panne qui risque d'affecter les dispositifs de sécurité du SYSTÈME. La prorogation de l'homologation du SYSTÈME dépend normalement du résultat satisfaisant de ces contrôles.

92. Tous les SYSTÈMES auxquels des dispositifs de sécurité ont été intégrés sont inspectés ou examinés périodiquement par la SAA. Pour les SYSTÈMES qui traitent des informations TRÈS SECRET UE/EU TOP SECRET ou d'une catégorie spéciale, les inspections sont effectuées au moins une fois par an.

Chapitre VIII

Utilisation temporaire ou occasionnelle

SÉCURITÉ DES MICRO-ORDINATEURS ET ORDINATEURS INDIVIDUELS

93. Les micro-ordinateurs et ordinateurs individuels (PC) dotés d'un disque dur fixe (ou d'autres supports à mémoire rémanente) et utilisés de façon autonome ou en réseau, ainsi que les machines portables (PC et blocs-notes électroniques, par exemple) équipées d'un disque dur fixe, sont considérés comme des supports d'informations au même titre que les disquettes ou autres supports informatiques amovibles.

94. Ces matériels reçoivent le niveau de protection, en termes d'accès, de manipulation, de rangement et de transport, qui convient au plus haut niveau de classification des informations stockées ou traitées (jusqu'à ce qu'elles soient déclassées ou déclassifiées suivant les procédures agréées).

UTILISATION DE MATÉRIEL TI PERSONNEL POUR UN TRAVAIL OFFICIEL DANS LE CADRE DU CONSEIL

95. Il est interdit d'utiliser des supports, logiciels et matériels TI personnels (par exemple PC et dispositifs électroniques portables) dotés d'une mémoire, pour traiter des informations classifiées de l'UE.

96. Aucun matériel, logiciel ou support personnel ne doit être introduit dans une zone de catégorie I ou II où sont traitées des informations classifiées de l'UE sans l'autorisation du chef du Bureau de sécurité du Conseil ou d'un service d'un État membre ou de l'organisme décentralisé de l'UE concerné.

UTILISATION DE MATÉRIEL TI APPARTENANT À UN CONTRACTANT OU FOURNI PAR UN PAYS POUR UN TRAVAIL OFFICIEL DANS LE CADRE DU CONSEIL

97. L'utilisation de matériel TI et de logiciels appartenant à un contractant pour effectuer au sein de l'organisation un travail officiel dans le cadre du Conseil peut être autorisée par le chef du Bureau de sécurité du SGC ou d'un service d'un État membre ou de l'organisme décentralisé de l'UE concerné. L'utilisation par des agents du Conseil ou d'un organisme décentralisé de l'UE de matériel TI et de logiciels fournis par un pays peut également être autorisée; dans ce cas, le matériel TI est inclus dans le système de pointage approprié du Conseil. En tout état de cause, si le matériel en question doit servir à traiter des informations classifiées de l'UE, il faut consulter la SAA appropriée, afin que les aspects INFOSEC applicables à l'utilisation de cet équipement soient dûment pris en compte et mis en œuvre.

SECTION XII

COMMUNICATION D'INFORMATIONS CLASSIFIÉES DE L'UE À DES ÉTATS TIERS OU À DES ORGANISATIONS INTERNATIONALES

PRINCIPES RÉGISSANT LA COMMUNICATION D'INFORMATIONS CLASSIFIÉES DE L'UE

1. La communication d'informations classifiées de l'UE à des États tiers ou à des organisations internationales est décidée par le Conseil sur la base:

   — de la nature et du contenu de ces informations,

   — du besoin d'en connaître des destinataires,

   — d'une appréciation des avantages à en attendre pour l'UE.

   L'accord préalable de l'État membre qui est à l'origine des informations classifiées à communiquer est sollicité.

2. Ces décisions sont prises au cas par cas en fonction:

   — du degré de coopération souhaité avec les États tiers ou les organisations internationales concernés,

   — de la confiance qui peut leur être accordée, laquelle résulte du niveau de la sécurité dont bénéficieraient les informations classifiées de l'UE confiées à ces États ou organisations ainsi que de la compatibilité entre les règles de sécurité qui y sont en vigueur et celles appliquées dans l'UE; le Comité de sécurité du Conseil fournit au Conseil un avis technique sur ce point.

3. L'acceptation par des États tiers ou des organisations internationales d'informations classifiées de l'UE implique l'assurance que ces informations ne seront pas utilisées à d'autres fins que celles qui ont motivé leur communication ou les échanges d'informations, et qu'ils leur assureront la protection requise par le Conseil.

LES NIVEAUX

4. Lorsque le Conseil décide que des informations classifiées peuvent être communiquées à tel État ou telle organisation internationale ou échangées avec eux, il arrête le niveau de coopération possible. Celui-ci dépend en particulier de la politique et de la réglementation de sécurité propres à cet État ou à cette organisation.

5. On distingue trois niveaux de coopération:

   Niveau 1

   Coopération avec des États tiers ou avec des organisations internationales dont la politique et la réglementation de sécurité sont très proches de celles de l'UE.

   Niveau 2

   Coopération avec des États tiers ou avec des organisations internationales dont la politique et la réglementation de sécurité sont sensiblement différentes de celles de l'UE.

   Niveau 3

   Coopération occasionnelle avec des États tiers ou avec des organisations internationales dont la politique et la réglementation de sécurité ne peuvent être appréciées.

6. Chaque niveau de coopération détermine les règles de sécurité, adaptées au cas par cas en fonction de l'avis technique du Comité de sécurité du Conseil, qu'il sera demandé aux bénéficiaires d'appliquer pour protéger les informations classifiées qui leur sont communiquées. Ces procédures et règles de sécurité sont exposées en détail aux annexes 4, 5 et 6.

LES ACCORDS

7. Lorsque le Conseil décide qu'il y a un besoin permanent ou durable d'échange d'informations classifiées entre l'UE et des États tiers ou d'autres organisations internationales, il élabore avec eux des «accords sur les procédures de sécurité pour l'échange d'informations classifiées» définissant l'objet de la coopération et les règles de protection réciproque des informations échangées.

8. Dans le cas des coopérations occasionnelles du niveau 3, qui sont par définition limitées dans le temps et dans leur objet, un simple mémorandum d'entente, définissant la nature des informations classifiées à échanger et les obligations réciproques à leur égard, peut se substituer à l'«accord sur les procédures pour l'échange d'informations classifiées», à condition que le niveau de classification de ces informations ne dépasse pas RESTREINT UE.

9. Les projets d'accords sur les procédures de sécurité ou de mémorandums d'entente sont approuvés par le Comité de sécurité avant présentation pour décision au Conseil.

10. Les ANS fournissent au Secrétaire général/Haut représentant toute l'aide nécessaire pour s'assurer que les informations communiquées sont utilisées et protégées conformément aux termes des accords sur les procédures de sécurité ou mémorandums d'entente.

Annexe 1

Liste des autorités nationales de sécurité

BELGIQUE

Ministère des Affaires Étrangères, du Commerce Extérieur et de la Coopération au Développement
Direction de la sécurité — A 01
Rue des Petits Carmes, 15
B-1000 Bruxelles
Téléphone: 32-2-501 85 14
Fax: 32-2-501 80 58
Télex: 21376
Adresse télégraphique: Direction de Sécurité A01 — MINAFET

DANEMARK

Politiets Efterretningstjeneste
Borups Alle 266
DK-2400 Copenhagen NV
Téléphone: 45-33 14 88 88
Fax: 45-38 19 07 05

Forsvarsministeriet
Forsvarets Efterretningstjeneste
Kastellet 30
DK-2100 Copenhagen Ø
Téléphone: 45-33 32 55 66
Fax: 45-33 93 13 20

ALLEMAGNE

Bundesministerium des Innern
Referat IS 4
Alt-Moabit 101D
D-10559 Berlin
Téléphone: 49-30-39 81 15 28
Fax: 49-30-39 81 16 10

GRÈCE

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Υπηρεσία Στρατιωτικών Πληροφοριών (ΥΣΠ - Β' Κλάδος)
Γραφείο Ασφάλειας
ΣΤΓ 1020-Χολαργός (Αθήνα)
Ελλαδα
Τηλέφωνα: 00 30-1-655 22 03 (ώρες γραφείου)
00 30-1-655 22 05 (εικοσιτετράωρο)
Φαξ: 00 30-1-642 69 40

Hellenic National Defence
General Staff (HNDGS)
Intelligence Branch/Security
(INT. BR./SEC.)
STG 1020, Holargos — Athens
Greece
Téléphone: 00 30-1-655 22 03 (heures de bureau)
00 30-1-655 22 05 (24 heures sur 24)
Fax: 00 30-1-642 69 40

ESPAGNE

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera Nacional Radial VI, km 8,500
E-28023 Madrid
Téléphone: 34-91-372 57 07
Fax: 34-91-372 58 08
E-mail: nsa-sp@areatec.com

FRANCE

Secrétariat général de la Défense Nationale
Service de Sécurité de Défense (SGDN/SSD)
51 Boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Téléphone: 33-0-144 18 81 80
Fax: 33-0-144 18 82 00
Télex: SEGEDEFNAT 200019
Adresse télégraphique: SEGEDEFNAT PARIS

IRLANDE

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
Dublin 2
Téléphone: 353-1-478 08 22
Fax: 353-1-478 14 84

ITALIE

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Ufficio Centrale per la Sicurezza
Via della Pineta Sacchetti, 216
I-00168 Roma
Téléphone: 39-06-627 47 75
Fax: 39-06-614 33 97
Télex: 623876 AQUILA 1
Adresse télégraphique: ess: PCM-ANS-UCSI-ROMA

LUXEMBOURG

Autorité Nationale de Sécurité
Ministère d'État
Boîte Postale 2379
L-1023 Luxembourg
Téléphone: 352-478 22 10 (central)
352-478 22 35 (direct)
Fax: 352-478 22 43
352-478 22 71
Télex: 3481 SERET LU
Adresse télégraphique: MIN D'ETAT — ANS

PAYS-BAS

Ministerie van Binnenlandse Zaken
Postbus 20010
NL-2500 EA Den Haag
Téléphone: 31-70-320 44 00
Fax: 31-70-320 07 33
Télex: 32166 SYTH NL

Ministerie van Defensie
Militaire Inlichtingendienst (MID)
Postbus 20701
NL-2500 ES Den Haag
Téléphone: 31-70-318 70 60
Fax: 31-70-318 79 51

AUTRICHE

Bundesministerium für auswärtige Angelegenheiten
Abteilung I.9
Ballhausplatz 2
A-1014 Wien
Téléphone: 43-1-531 15 34 64
Fax: 43-1-531 8 52 19

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1449-004 Lisboa
Téléphone: 351-21-301 55 10
351-21-301 00 01, poste 20 45 37
Fax: 351-21-302 03 50

FINLANDE

Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Ulkoasiainministeriö/Utrikesministeriet
Laivastokatu/Maringatan 22
PL/PB 176
FIN-00161 Helsinki/Helsingfors
Téléphone: 358-9-13 41 53 38
Fax: 358-9-13 41 53 03

SUÈDE

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Téléphone: 46-8-405 54 44
Fax: 46-8-723 11 76

ROYAUME-UNI

The Secretary (for DIR/5)
PO Box 5656
London EC1A 1AH
Téléphone: 44-20-72 70 87 51
Fax: 44-20-76 30 14 28
Adresse télégraphique: UK Delegation to Security Policy Department FCO, en indiquant la mention: «in Box 5656 for DIR/5».

Annexe 2

Tableau comparatif des classifications de sécurité nationales

Classification UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Classification OTAN ([1])				
Classification UEO	FOCAL Très secret	UEO Secret	UEO Confidential	UEO Restreint
Belgique	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Danemark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Allemagne	STRENG GEHEIM	GEHEIM	VS ([2]) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Grèce	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Espagne	Secreto	Reservado	Confidencial	Difusion Limitada
France	Très Secret Défense ([3])	Secret Défense	Confidentiel Défense	Diffusion restreinte
Irlande	Top Secret	Secret	Confidential	Restricted
Italie	Segretissimo	Segreto	Riservatissimo	Riservato
Luxembourg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Pays-Bas	STG Zeer Geheim	STG Geheim	STG Confidentieel	
Autriche	Streng geheim	Geheim	Vertraulich	Eingeschränkt
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Finlande	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Suède	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Royaume-Uni	Top Secret	Secret	Confidential	Restricted

([1]) OTAN: la correspondance avec les niveaux de classification de l'OTAN sera établie lors de la négociation de l'accord de sécurité entre l'Union européenne et l'OTAN.
([2]) Allemagne: VS = Verschlusssache.
([3]) France: la classification Très Secret Défense, couvrant les priorités gouvernementales, ne peut s'échanger qu'avec l'autorisation du premier ministre.

Annexe 3

Guide pratique de la classification

Le présent guide a un caractère indicatif et ne peut être interprété comme modifiant les dispositions de fond énoncées aux sections II et III.

Classification	Quand	Qui	Timbres	Déclassement/déclassification/destruction	
				Qui	Quand
TRÈS SECRET UE/ EU TOP SECRET: Cette classification s'applique exclusivement aux 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 [SII, § 1].	La compromission d'informations ou de matériels portant la mention TRÈS SECRET UE/EU TOP SECRET risquerait de: — menacer directement la stabilité interne de l'UE ou de l'un de ses États membres ou pays amis — causer un préjudice exceptionnellement grave aux relations avec des gouvernements amis — entraîner directement la perte d'un grand nombre de vies humaines — causer un préjudice exceptionnellement grave à l'efficacité opérationnelle ou à la sécurité des forces armées des États membres ou d'autres contributeurs, ou au maintien de l'efficacité d'opérations de sécurité ou de renseignement extrêmement utiles — causer un grave préjudice à long terme à l'économie de l'UE ou des États membres.	États membres: personnes dûment autorisées (autorités d'origine) [SIII, § 4]; SGC: personnes dûment autorisées (autorités d'origine) [SIII, § 4], SG/HR et SGA Les autorités d'origine fixent une date ou un délai à partir duquel les informations contenues dans un document pourront être déclassées ou déclassifiées. Sinon, elles réexaminent la question tous les cinq ans au plus pour s'assurer que la classification initiale reste nécessaire [SIII, § 10].	La classification TRÈS SECRET UE/EU TOP SECRET est apposée sur les documents TRÈS SECRET UE/EU TOP SECRET et entraîne, le cas échéant, l'apposition du timbre défense PESD, par voie mécanique et à la main [SII, § 8]. Les classifications UE doivent apparaître au milieu de chaque page, en haut et en bas, et chaque page doit être numérotée. Chaque document doit porter un numéro de référence ainsi qu'une date; ce numéro de référence figurera sur chaque page. S'ils doivent être diffusés en plusieurs exemplaires, chacun d'eux devra porter un numéro d'exemplaire qui figurera en première page, avec le nombre total de pages. La première page d'un document doit donner la liste complète des annexes et pièces jointes [SVII, § 1].	La décision de déclassifier ou de déclasser un document revient exclusivement à l'autorité d'origine, ou au SG/HR ou SGA, qui doivent informer du changement de classification les destinataires successifs auxquels ils ont fait suivre l'original ou une copie du document [SIII, § 9]. Les documents TRÈS SECRET UE/EU TOP SECRET sont détruits par le bureau d'ordre central ou subordonné qui en a la charge. La destruction de chaque document est inscrite sur un procès-verbal de destruction, signé par l'agent contrôleur TRÈS SECRET UE/EU TOP SECRET et par l'agent qui a été témoin de la destruction et qui doit être habilité TRÈS SECRET UE/EU TOP SECRET. Le cahier d'enregistrement comportera une note à cet effet. Le bureau d'ordre doit conserver pendant dix ans les procès-verbaux de destruction, ainsi que la fiche de circulation [SVII, § 31].	Les exemplaires excédentaires et les documents jugés périmés doivent être détruits [SVII, § 31]. Les documents TRÈS SECRET UE/EU TOP SECRET, y compris tous les rebuts classifiés résultant de l'élaboration des documents TRÈS SECRET UE/EU TOP SECRET (exemplaires endommagés, brouillons, notes dactylographiées, papiers carbones, etc.), doivent être détruits sous la surveillance d'un responsable habilité TRÈS SECRET UE/EU TOP SECRET, par incinération, réduction en pulpe, lacération en bandes ou division en fragments non identifiables rendant impossible toute reconstitution [SVII, § 31].

Classification	Quand	Qui	Timbres	Déclassement/déclassification/destruction	
				Qui	Quand
SECRET UE Cette classification s'applique uniquement aux 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 [SII, § 2]	La compromission d'informations ou de matériels portant la mention SECRET UE risquerait de: — provoquer des tensions internationales — nuire gravement aux relations avec des gouvernements amis — menacer directement des vies humaines ou de nuire gravement à l'ordre public ou à la sécurité ou à la liberté des personnes — nuire gravement à l'efficacité opérationnelle ou à la sécurité des forces armées des États membres ou d'autres contributeurs, ou au maintien de l'efficacité d'opérations de sécurité ou de renseignement très utiles — causer un préjudice matériel important aux intérêts financiers, monétaires, économiques et commerciaux de l'UE ou de l'un de ses États membres.	États membres: personnes autorisées (autorités d'origine) [SIII, § 2]; SGC et organismes décentralisés de l'UE: personnes autorisées (autorités d'origine) [SIII, § 2], Directeurs généraux, SG/HR et SGA Les autorités d'origine fixent une date ou un délai à partir duquel les informations contenues dans un document pourront être déclassées ou déclassifiées. Sinon, elles réexaminent la question tous les cinq ans au plus pour s'assurer que la classification initiale reste nécessaire [SIII, § 10].	La classification SECRET UE est apposée sur les documents SECRET UE et entraîne, le cas échéant, l'apposition du timbre défense PESD, par voie mécanique et à la main [SII, § 8]. Les classifications UE doivent apparaître au milieu de chaque page, en haut et en bas, et chaque page doit être numérotée. Chaque document doit porter un numéro de référence ainsi qu'une date; ce numéro de référence figurera sur chaque page. S'ils doivent être diffusés en plusieurs exemplaires, chacun d'eux devra porter un numéro d'exemplaire qui figurera en première page, avec le nombre total de pages. La première page d'un document doit donner la liste complète des annexes et pièces jointes [SVII, § 1].	La décision de déclassifier ou de déclasser un document revient exclusivement à l'autorité d'origine, ou au SG/HR ou SGA, qui doivent informer du changement de classification les destinataires auxquels ils ont fait suivre l'original ou une copie du document [SIII, § 9]. Les documents SECRET UE sont détruits par le bureau d'ordre qui en a la charge, sous la surveillance d'une personne possédant une habilitation de sécurité. Les documents SECRET UE qui sont détruits sont inscrits sur des procès-verbaux de destruction signés que le bureau d'ordre doit conserver, de même que la fiche de circulation, pendant au moins trois ans [SVII, § 32].	Les exemplaires excédentaires et les documents jugés périmés doivent être détruits [SVII, § 31]. Les documents SECRET UE, y compris tous les rebuts classifiés résultant de l'élaboration des documents SECRET UE (exemplaires endommagés, brouillons, notes dactylographiées, papiers carbones, etc.), doivent être détruits par incinération, réduction en pulpe, lacération en bandes ou division en fragments non identifiables rendant impossible toute reconstitution [SVII, § 31 et 32].

Classification	Quand	Qui	Timbres	Déclassement/déclassification/destruction	
				Qui	Quand
CONFIDENTIEL UE Cette classification s'applique aux informations et matériels dont la divulgation non autorisée nuirait aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres [SII, § 3].	La compromission d'informations ou de matériels portant la mention CONFIDENTIEL UE risquerait de: — causer un préjudice important aux relations diplomatiques, c'est-à-dire de donner lieu à des protestations officielles ou autres sanctions — porter préjudice à la sécurité ou à la liberté des personnes — nuire à l'efficacité opérationnelle ou à la sécurité des forces armées des États membres ou d'autres contributeurs, ou à l'efficacité d'opérations de sécurité ou de renseignement utiles — compromettre de manière substantielle la viabilité financière de grandes organisations — faire obstacle aux enquêtes relatives à des infractions graves ou faciliter la commission de ces infractions — aller fortement à l'encontre des intérêts financiers, monétaires, économiques et commerciaux de l'UE ou de ses États membres — entraver gravement l'élaboration ou le fonctionnement des principales politiques de l'UE — faire cesser ou de perturber fortement d'une manière quelconque des activités importantes de l'UE.	États membres: personnes autorisées (autorités d'origine) [SIII, § 2]; SGC et organismes décentralisés de l'UE: personnes autorisées (autorités d'origine) [SIII, § 2], Directeurs généraux, SG/HR et SGA. Les autorités d'origine fixent une date ou un délai à partir duquel les informations contenues dans un document pourront être déclassées ou déclassifiées. Sinon, elles réexaminent la question tous les cinq ans au plus pour s'assurer que la classification initiale reste nécessaire [SIII, § 10].	La mention de classification CONFIDENTIEL UE est apposée sur les documents CONFIDENTIEL UE et entraîne; le cas échéant, l'apposition du timbre de la défense PESD, par voie mécanique et à la main ou par impression sur du papier portant un cachet pré-imprimé et enregistré [SII, § 8]. Les classifications UE doivent apparaître au milieu de chaque page, en haut et en bas, et chaque page doit être numérotée. Chaque document doit porter un numéro de référence ainsi qu'une date. La première page d'un document doit donner la liste complète des annexes et pièces jointes [SVII, § 1].	La décision de déclassifier ou de déclasser un document revient exclusivement à l'autorité d'origine ou au SG/HR ou SGA, qui doivent informer du changement de classification les destinataires successifs auxquels ils ont fait suivre l'original ou une copie du document [SIII, § 31]. Les documents CONFIDENTIEL UE sont détruits par le bureau d'ordre qui en a la charge, sous la surveillance d'une personne habilitée. Leur destruction est enregistrée conformément aux réglementations nationales et, dans le cas du SGC ou des organismes décentralisés de l'UE, conformément aux instructions du SG/HR ou SGA [SVII, § 33].	Les exemplaires excédentaires et les documents jugés périmés doivent être détruits [SVII, § 31]. Les documents CONFIDENTIEL UE, y compris tous les rebuts classifiés résultant de l'élaboration des documents CONFIDENTIEL UE (exemplaires endommagés, brouillons, notes dactylographiées, papiers carbones, etc.), doivent être détruits par incinération, réduction en pulpe, lacération en bandes ou division en fragments non identifiables rendant impossible toute reconstitution [SVII, § 31 et 33].

Classification	Quand	Qui	Timbres	Déclassement/déclassification/destruction	
				Qui	Quand
RESTREINT UE: Cette classification s'applique aux 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 [SII, § 4].	La compromission d'informations ou de matériels portant la mention RESTREINT UE risquerait de: — nuire aux relations diplomatiques — causer des souffrances importantes à des personnes — rendre l'efficacité opérationnelle ou la sécurité des forces armées des États membres ou d'autres contributeurs plus difficile à maintenir — causer des pertes financières ou de faciliter l'obtention de gains ou d'avantages indus par des personnes ou des sociétés — violer des engagements pris en bonne et due forme de préserver la confidentialité d'informations fournies par des tiers — enfreindre les restrictions légales à la divulgation d'informations — nuire aux enquêtes relatives à des infractions ou faciliter la commission de ces infractions — faire tort à l'UE ou à ses États membres dans des négociations commerciales ou stratégiques — entraver l'élaboration ou le fonctionnement efficaces des politiques de l'UE — compromettre la bonne gestion de l'UE et de ses activités.	États membres: personnes autorisées (autorités d'origine) [SIII, § 2]; SGC et organismes décentralisés de l'UE: personnes autorisées (autorités d'origine) [SIII, § 2], Directeurs généraux, SG/HR et SGA Les autorités d'origine fixent une date ou un délai à partir duquel les informations contenues dans un document pourront être déclassées ou déclassifiées. Sinon, elles réexaminent la question tous les cinq ans au plus pour s'assurer que la classification initiale reste nécessaire [SIII, § 10].	La classification RESTREINT UE est apposée sur les documents RESTREINT UE et entraîne, le cas échéant, l'apposition du timbre de la défense PESD, par voie mécanique ou électronique [SII, § 8]. Les classifications UE doivent apparaître au milieu de chaque page, en haut et en bas, et chaque page doit être numérotée. Chaque document doit porter un numéro de référence ainsi qu'une date [SVII, § 1].	La décision de déclassifier ou de déclasser un document revient exclusivement à l'autorité d'origine ou au SG/HR ou SGA, qui doivent informer du changement de classification les destinataires auxquels ils ont fait suivre l'original ou une copie du document [SIII, § 9]. Les documents RESTREINT UE sont détruits par le bureau d'ordre qui en a la charge, conformément aux réglementations nationales et, dans le cas du SGC ou des organismes décentralisés de l'UE, conformément aux instructions du SG/HR ou SGA [SVII, § 34].	Les exemplaires excédentaires et les documents jugés périmés doivent être détruits [SVII, § 31].

Annexe 4

Lignes directrices concernant la communication d'informations classifiées de l'UE à des États tiers ou à des organisations internationales

Niveau 1 de coopération

PROCÉDURES

1. La communication d'informations classifiées de l'UE à des pays non signataires du traité sur l'Union européenne ou autres organisations internationales dont la politique et la réglementation de sécurité sont comparables à celles de l'UE est du ressort du Conseil.

2. Le Conseil peut déléguer la décision de communication d'informations classifiées de l'UE. La délégation précise la nature des informations communicables et leur niveau de classification, limité normalement à CONFIDENTIEL UE.

3. Sous réserve de la conclusion d'un accord de sécurité, les demandes de communication d'informations classifiées de l'UE sont introduites auprès du Secrétaire général/Haut représentant par les services responsables de la sécurité des pays ou organisations internationales concernés, qui précisent à quelles fins cette communication est destinée et la nature des informations classifiées souhaitées.

   Elles peuvent l'être également par les États membres ou les organismes décentralisés de l'UE estimant souhaitable la communication d'informations classifiées de l'UE; les demandeurs précisent les fins et l'avantage pour l'UE de cette communication, ainsi que la nature et le degré de classification des informations à communiquer.

4. La demande est instruite par le SGC, qui:

   — recueille l'avis de l'État membre ou, le cas échéant, de l'organisme décentralisé de l'UE qui est à l'origine des informations à communiquer,

   — établit les contacts nécessaires avec les services responsables de la sécurité des pays ou des organisations internationales bénéficiaires, pour vérifier que leur politique et leur réglementation de sécurité garantissent que les informations classifiées communiquées seront protégées conformément au présent règlement de sécurité,

   — recueille auprès des autorités nationales de sécurité des États membres leur avis technique sur la confiance que l'on peut accorder aux pays ou organismes internationaux bénéficiaires.

5. Le SGC transmet pour décision au Conseil la demande et la recommandation du Bureau de sécurité.

RÈGLES DE SÉCURITÉ À APPLIQUER PAR LES BÉNÉFICIAIRES

6. La décision du Conseil d'autoriser la communication d'informations classifiées de l'UE est portée à la connaissance des États ou des organisations internationales bénéficiaires par le Secrétaire général/Haut représentant, accompagnée du nombre d'exemplaires du présent règlement de sécurité jugé nécessaire. Si la demande émane d'un État membre, l'autorisation de communication est portée à la connaissance du bénéficiaire par cet État.

   Elle ne devient exécutoire que lorsque les bénéficiaires se sont engagés par écrit:

   — à ne pas utiliser les informations à d'autres fins que celles qui ont été arrêtées,

   — à les protéger conformément au présent règlement de sécurité et notamment aux dispositions particulières ci-après.

7. *Personnel*

   a) Le nombre des agents ayant accès aux informations classifiées de l'UE est strictement limité, selon le principe du besoin d'en connaître, aux seules personnes dont les fonctions exigent l'accès à ces informations.

b) Tout agent ou ressortissant autorisé à avoir accès aux informations classifiées CONFIDENTIEL UE ou d'un niveau de classification plus élevé doit être titulaire soit d'un certificat de sécurité du niveau approprié, soit d'une habilitation de sécurité de niveau équivalent; l'un ou l'autre sont délivrés par le gouvernement de son État d'appartenance.

8. *Transmission des documents*

a) Les modalités pratiques de transmission des documents sont arrêtées d'un commun accord sur la base des prescriptions de la section VII du présent règlement de sécurité. Elles précisent en particulier à quels bureaux d'ordre sont transmises les informations classifiées de l'UE.

b) Si la communication d'informations classifiées de l'UE autorisée par le Conseil inclut le niveau TRÈS SECRET UE/EU TOP SECRET, le pays ou l'organisation internationale bénéficiaire doit ouvrir un bureau d'ordre UE central et, si besoin est, des bureaux d'ordre UE subordonnés. Ces bureaux d'ordre sont régis par les dispositions de la section VIII du présent règlement de sécurité.

9. *Enregistrement*

Dès qu'un bureau d'ordre reçoit un document UE classifié CONFIDENTIEL UE ou au-dessus, il l'inscrit dans un registre spécial tenu par l'organisation et divisé en colonnes indiquant la date de réception du document, sa référence (date, cote et numéro d'exemplaire), sa classification, son objet, le nom ou la fonction du destinataire, la date de renvoi du reçu ainsi que la date de renvoi du document à l'autorité d'origine au sein de l'UE ou de sa destruction.

10. *Destruction*

a) La destruction des documents classifiés de l'UE s'effectue conformément aux instructions figurant à la section VI du présent règlement de sécurité. Des copies des procès-verbaux de destruction des documents SECRET UE et TRÈS SECRET UE/EU TOP SECRET sont adressées au bureau d'ordre expéditeur de l'UE.

b) Les documents classifiés de l'UE doivent être compris dans les plans de destruction d'urgence des documents classifiés des services bénéficiaires.

11. *Protection des documents*

Toute disposition doit être prise pour empêcher l'accès aux informations classifiées de l'UE par des personnes non autorisées.

12. *Copies, traductions et extraits*

Il est interdit de photocopier un document classifié CONFIDENTIEL UE ou SECRET UE, d'en faire des traductions ou d'en extraire des passages, sans l'autorisation du chef de l'organisation de sécurité concernée qui enregistrera et contrôlera les copies, les traductions ou les extraits et y apposera les timbres nécessaires.

La reproduction ou la traduction d'un document TRÈS SECRET UE/EU TOP SECRET ne peut être autorisée que par l'autorité d'origine qui indiquera le nombre de copies autorisées; si l'autorité d'origine ne peut être déterminée, la question est renvoyée au Bureau de sécurité du SGC.

13. *Infractions à la sécurité*

Lorsque l'on constate ou que l'on soupçonne qu'une infraction à la sécurité a été commise et qu'elle met en cause un document classifié de l'UE, il convient de prendre immédiatement les mesures ci-après, sous réserve de la conclusion d'un accord de sécurité:

a) mener une enquête pour établir les circonstances de l'infraction;

b) avertir le Bureau de sécurité du SGC, l'ANS et l'autorité d'origine, ou bien préciser, le cas échéant, que cette dernière n'a pas été avertie;

c) faire en sorte de limiter au minimum les incidences de cette infraction;

d) réexaminer et mettre en œuvre les mesures propres à empêcher toute récidive;

e) mettre en œuvre toute recommandation du Bureau de sécurité du SGC propre à empêcher une récidive.

14. *Inspections*

Le Bureau de sécurité du SGC est autorisé à effectuer, en accord avec les États ou organisations internationales concernés, des vérifications de l'efficacité des mesures de protection des informations classifiées de l'UE communiquées.

15. *Rapports*

Sous réserve de la conclusion d'un accord de sécurité, tant que le pays ou l'organisation internationale détient des informations classifiées de l'UE, il doit soumettre chaque année, à une date fixée lorsque l'autorisation lui est donnée de recevoir ces informations, un rapport confirmant que le présent règlement de sécurité est respecté.

Annexe 5

Lignes directrices concernant la communication d'informations classifiées de l'UE à des États tiers ou à des organisations internationales

Niveau 2 de coopération

PROCÉDURES

1. La communication d'informations classifiées de l'UE à des États tiers ou à des organisations internationales dont la politique et la réglementation de sécurité sont sensiblement différentes de celles de l'UE est du ressort du Conseil. Elle est, en principe, limitée aux informations classifiées jusqu'au niveau SECRET UE inclus; en sont exclues, les informations nationales communiquées aux seuls États membres et les catégories d'informations classifiées de l'UE protégées par des timbres spéciaux.

2. Le Conseil peut déléguer sa décision; la délégation, qui s'inscrit dans le cadre des limitations définies au point 1, précise la nature des informations communicables et leur degré de classification, limité à RESTREINT UE.

3. Sous réserve de la conclusion d'un accord de sécurité, les demandes de communication d'informations classifiées de l'UE sont introduites auprès du Secrétaire général/Haut représentant par les services responsables de la sécurité des États ou organisations internationales concernés, qui précisent à quelles fins cette communication est destinée ainsi que la nature et la classification des informations souhaitées.

   Elles peuvent l'être également par les États membres ou les organismes décentralisés de l'UE estimant souhaitable la communication d'informations classifiées de l'UE; les demandeurs précisent les fins et l'avantage pour l'UE de cette communication, ainsi que la nature et la classification des informations à communiquer.

4. La demande est instruite par le SGC, qui:

   — recueille l'avis de l'État membre ou, le cas échéant, de l'organisme décentralisé de l'UE qui est à l'origine des informations à communiquer,

   — établit des contacts préliminaires avec les services responsables de la sécurité des États ou organisations internationales bénéficiaires, pour s'informer sur leur politique et leur réglementation de sécurité et en particulier établir un tableau d'équivalence des degrés de classification en vigueur dans l'UE et dans l'État ou l'organisation concerné(e),

   — organise une réunion du Comité de sécurité du Conseil ou interroge, par procédure de silence le cas échéant, les autorités nationales de sécurité des États membres en vue de recueillir l'avis technique du Comité de sécurité.

5. L'avis technique du Comité de sécurité du Conseil porte sur les éléments suivants:

   — confiance à accorder aux États ou aux organisations internationales bénéficiaires afin d'évaluer les risques de sécurité encourus par l'UE ou ses États membres,

   — évaluation de la capacité des bénéficiaires à assurer la protection des informations classifiées communiquées par l'UE,

   — propositions concernant les modalités pratiques de traitement des informations classifiées de l'UE (expurgation du texte, par exemple) et des documents transmis (maintien ou suppression des mentions de classification UE, marquage spécifique, etc.),

   — déclassement ou déclassification préalable par l'autorité d'origine des informations avant leur communication aux pays ou organisations internationales bénéficiaires ([1]).

([1]) Ce qui entraîne l'application par l'autorité d'origine de la procédure définie au point 9 de la section III pour tous les exemplaires diffusés au sein de l'UE.

6. Le Secrétaire général/Haut représentant transmet pour décision au Conseil la demande et l'avis technique du Comité de sécurité du Conseil recueilli par le Bureau de sécurité du SGC.

RÈGLES DE SÉCURITÉ À APPLIQUER PAR LES BÉNÉFICIAIRES

7. La décision du Conseil d'autoriser la communication d'informations classifiées de l'UE est portée à la connaissance des pays ou organisations internationales bénéficiaires par le Secrétaire général/Haut représentant, accompagnée d'un tableau d'équivalence des degrés de classification en vigueur à l'UE et dans les États ou les organisations concernés. Si la demande émane d'un État membre, l'autorisation de communication est portée à la connaissance du bénéficiaire par cet État.

   Elle ne devient exécutoire que lorsque les bénéficiaires se sont engagés par écrit:

   — à ne pas utiliser les informations communiquées à d'autres fins que celles qui ont été arrêtées,

   — à les protéger conformément aux règles fixées par le Conseil.

8. Les règles de protection suivantes sont établies pour le cas où aucune procédure particulière de traitement des documents classifiés de l'UE (suppression de la mention de classification UE, marquage spécifique, etc.) n'a été arrêtée par le Conseil sur avis technique du Comité de sécurité.

   Elles sont à adapter dans le cas contraire.

9. *Personnel*

   a) Le nombre des agents ayant accès aux informations classifiées de l'UE doit être strictement limité, selon le principe du besoin d'en connaître, aux seules personnes dont les fonctions exigent l'accès à ces informations.

   b) Tout agent ou ressortissant autorisé à avoir accès aux informations classifiées communiquées par l'UE doit être titulaire d'une habilitation ou d'une attestation de sécurité nationale lui autorisant l'accès, en ce qui concerne les informations classifiées nationales, au degré approprié équivalent à celui de l'UE, tel que défini dans le tableau d'équivalence.

   c) Ces habilitations ou attestations de sécurité nationales sont communiquées pour information au Secrétaire général/Haut représentant.

10. *Transmission des documents*

   a) Les modalités pratiques de transmission des documents sont arrêtées en commun entre le Bureau de sécurité du SGC et les services responsables de la sécurité des États ou des organisations internationales destinataires, sur la base des règles établies par la section VII du présent règlement de sécurité. Elles indiquent en particulier les adresses précises auxquelles les documents doivent être envoyés ainsi que les services de courrier ou de messagerie utilisés pour la transmission des informations classifiées de l'UE.

   b) Les documents CONFIDENTIEL UE et d'un degré de classification plus élevé sont transmis sous double enveloppe. L'enveloppe intérieure porte la mention «UE» et celle de la classification du document. Une formule de récépissé est jointe à chaque document classifié. Elle n'a pas de classification et fournit exclusivement les références (cote, date, numéro d'exemplaire) et la langue du document, sans en indiquer l'objet.

   c) Cette enveloppe intérieure est ensuite glissée dans l'enveloppe extérieure, qui porte un numéro d'expédition en vue des formalités de réception. La classification du document ne doit pas figurer sur l'enveloppe extérieure.

   d) Un reçu portant le numéro d'expédition doit dans tous les cas être remis aux courriers.

11. *Enregistrement à l'arrivée*

   L'ANS du pays destinataire, ou son équivalent, qui prend en compte, au nom de son gouvernement, les informations classifiées communiquées par l'UE, ou le bureau de sécurité de l'organisation internationale destinataire, ouvre un registre spécial où sont enregistrés, dès réception, les documents classifiés de l'UE. Le registre est divisé en colonnes indiquant la date de réception du document, ses références (cote, date, numéro d'exemplaire), sa classification, son objet, le nom ou la fonction du destinataire, la date de renvoi du reçu et la date de renvoi du document à l'UE ou de sa destruction.

12. *Retour des documents*

Lorsque le destinataire renvoie un document classifié au Conseil ou à l'État membre qui l'a communiqué, il procède comme indiqué au point 10.

13. *Protection*

a) Lorsqu'ils ne sont pas utilisés, les documents sont enfermés dans un meuble de sécurité homologué pour le stockage des documents nationaux du même degré de classification. Ce meuble ne portera aucune indication de son contenu, dont seules peuvent prendre connaissance les personnes habilitées à traiter des informations classifiées de l'UE. S'il est muni d'une serrure à combinaison, celle-ci n'est connue que des agents de l'État ou de l'organisation autorisés à accéder aux informations classifiées de l'UE conservées dans le meuble; elle est changée tous les six mois, ou plus tôt en cas de transfert d'un agent, d'annulation de l'habilitation de sécurité d'un des agents qui connaît la combinaison ou de risque de compromission.

b) Seuls les agents habilités à accéder aux documents classifiés de l'UE et ayant le besoin d'en connaître sont autorisés à les retirer du meuble de sécurité. Ils doivent en assurer la surveillance tant qu'ils les ont en leur possession, et faire en sorte notamment qu'aucune personne non habilitée ait accès à ces documents. Ils doivent, en outre, veiller à les ranger dans un meuble de sécurité lorsqu'ils ont fini de les consulter et en dehors des heures de travail.

c) Il est interdit de photocopier un document CONFIDENTIEL UE et au-dessus, ou d'en tirer des extraits sans l'autorisation du Bureau de sécurité du SGC.

d) Il convient de définir et de confirmer avec le Bureau de sécurité du SGC la procédure à suivre pour la destruction rapide et totale des documents en cas d'urgence.

14. *Sécurité physique*

a) Lorsqu'il n'est pas utilisé, un meuble de sécurité abritant des documents classifiés de l'UE doit être en permanence fermé à clé.

b) Le personnel d'entretien ou de nettoyage devant pénétrer ou travailler dans un local abritant des meubles de sécurité est en permanence escorté par un membre des services de sécurité de l'État ou de l'organisation, ou par l'agent plus particulièrement chargé de veiller à la sécurité de ce local.

c) En dehors des heures de travail normales (la nuit, en fin de semaine et pendant les congés), la protection du meuble de sécurité contenant des documents classifiés de l'UE est assurée soit par un garde soit par un système d'alarme automatique.

15. *Infractions à la sécurité*

Lorsque l'on constate ou que l'on soupçonne qu'une infraction à la sécurité a été commise et met en cause un document classifié de l'UE, il convient de prendre sur-le-champ les mesures suivantes:

a) adresser immédiatement un rapport au Bureau de sécurité du SGC ou à l'ANS de l'État membre ayant pris l'initiative de communiquer les documents (avec copie au Bureau de sécurité du SGC);

b) effectuer une enquête, à l'issue de laquelle un rapport complet est soumis au service de sécurité [voir a) du présent point]. Les mesures requises pour remédier à la situation doivent ensuite être prises.

16. *Inspections*

Le Bureau de sécurité du SGC est autorisé à effectuer, en accord avec les États ou organisations internationales concernés, des vérifications de l'efficacité des mesures de protection des informations classifiées de l'UE communiquées.

17. *Rapports*

Tant que l'État ou l'organisation détient des informations classifiées de l'UE, il doit soumettre chaque année, à une date fixée lorsque l'autorisation lui est donnée de recevoir ces informations, un rapport confirmant que le présent règlement de sécurité est respecté.

Annexe 6

Lignes directrices concernant la communication d'informations classifiées de l'UE à des États tiers ou à des organisations internationales

Niveau 3 de coopération

PROCÉDURES

1. Il peut se produire que le Conseil décide de coopérer, dans certaines circonstances particulières, avec des États ou des organisations ne pouvant fournir les garanties exigées aux termes du présent règlement de sécurité: une telle coopération peut pourtant nécessiter la communication d'informations classifiées de l'UE. Les informations nationales spécifiquement réservées aux États membres sont alors exclues d'une telle communication.

2. Dans ces circonstances particulières, les demandes de coopération avec l'UE, qu'elles émanent d'États tiers ou d'organisations internationales ou soient proposées par les États membres ou des organismes décentralisés de l'UE, sont au préalable examinées au fond par le Conseil qui doit, le cas échéant, recueillir l'avis de l'État membre ou de l'organisme décentralisé qui est à l'origine des informations. Le Conseil juge de l'opportunité de la communication d'informations classifiées, apprécie le besoin d'en connaître des bénéficiaires et arrête la nature des informations classifiées communicables.

3. Si le Conseil émet un avis favorable, il incombe au Secrétaire général/Haut représentant de convoquer le Comité de sécurité du Conseil, ou d'interroger, éventuellement par procédure de silence, les autorités nationales de sécurité des États membres pour obtenir l'avis technique du Comité de sécurité.

4. L'avis technique du Comité de sécurité du Conseil porte sur les éléments suivants:

   a) évaluation des risques de sécurité encourus par l'UE ou ses États membres;

   b) degré de classification des informations communicables, éventuellement selon leur nature;

   c) déclassement ou déclassification préalable par l'autorité origine des informations avant communication aux pays ou organisations internationales concernés ([1]);

   d) modalités de traitement des documents à communiquer (voir point 5 ci-après);

   e) modes de communication possibles (utilisation des services postaux publics, des réseaux de télécommunication publics ou protégés, courrier diplomatique, courriers habilités, etc.).

5. Les documents communiqués aux États ou organisations visés par la présente annexe sont préparés, en principe, sans indiquer de référence d'origine ni mention de classification UE. Le Comité de sécurité du Conseil peut recommander:

   — l'adoption d'un timbre spécifique ou d'un nom code,

   — l'adoption d'un système de classification spécifique établissant un lien entre les différents degrés de sensibilité des informations communiquées et les mesures de contrôle exigées des bénéficiaires et les modes de communication des documents (voir exemples au point 14).

6. Le Bureau de sécurité du SGC soumet au Conseil l'avis technique du Comité de sécurité, en y joignant, si nécessaire, les propositions de délégation de pouvoir nécessaires à l'exécution de la mission, notamment en cas d'urgence.

7. Dès que la communication d'informations classifiées de l'UE et que les modalités pratiques d'exécution sont approuvées par le Conseil, le Bureau de sécurité du Conseil établit les contacts nécessaires avec le service de sécurité de l'État ou de l'organisation concernés pour faciliter l'application des dispositions de sécurité prévues.

([1]) Ce qui entraîne l'application par l'autorité d'origine de la procédure définie au point 9 de la section III pour tous les exemplaires diffusés au sein de l'UE.

8. ¡ titre de référence, le Bureau de sécurité du SGC diffuse à tous les États membres et, le cas échéant, organismes décentralisés de l'UE un tableau récapitulant la nature, le degré de classification des informations et les organisations et pays auxquels elles peuvent être communiquées, selon les décisions du Conseil.

9. L'ANS de l'État membre qui communique les informations, ou le Bureau de sécurité du SGC, prend toute mesure nécessaire pour faciliter l'évaluation du dommage et les révisions de procédures ultérieures éventuelles.

10. Le Conseil est saisi à nouveau chaque fois que les conditions de coopération sont modifiées.

RÈGLES DE SÉCURITÉ À APPLIQUER PAR LES BÉNÉFICIAIRES

11. La décision du Conseil d'autoriser la communication d'informations classifiées de l'UE est portée à la connaissance des États ou organisations internationales bénéficiaires par le Secrétaire général/Haut représentant, accompagnée des règles de protection détaillées proposées par le Comité de sécurité du Conseil et approuvées par le Conseil. Si la demande émane d'un État membre, l'autorisation de communication est portée à la connaissance du bénéficiaire par cet État.

Elle ne devient exécutoire que lorsque les bénéficiaires se sont engagés par écrit:

— à n'utiliser les informations communiquées qu'aux fins de la coopération décidée par le Conseil,

— à leur assurer la protection exigée par le Conseil.

12. *Transmission des documents*

a) Les modalités pratiques de transmission des documents sont arrêtées en commun entre le Bureau de sécurité du SGC et les services responsables de la sécurité des États ou organisations internationales destinataires. Elles indiquent en particulier les adresses précises auxquelles les documents doivent être envoyés.

b) Les documents classifiés CONFIDENTIEL UE et d'un degré de classification plus élevé sont transmis sous double enveloppe. L'enveloppe intérieure porte le timbre spécifique ou le nom de code retenu et la mention de la classification particulière agréée du document. Une formule de récépissé est jointe à chaque document classifié. La formule de récipissé n'a pas de classification et donne exclusivement les références (cote, date, numéro d'exemplaire) et la langue du document, sans en indiquer l'objet.

c) L'enveloppe intérieure est ensuite glissée dans l'enveloppe extérieure, qui porte un numéro d'expédition en vue des formalités de réception. Aucune classification de sécurité ne doit figurer sur l'enveloppe extérieure.

d) Un reçu portant le numéro d'expédition doit dans tous les cas être remis aux courriers.

13. *Enregistrement à l'arrivée*

L'ANS de l'État destinataire, ou son équivalent, qui prend en compte, au nom de son gouvernement, les informations classifiées communiquées par l'UE, ou le Bureau de sécurité de l'organisation internationale destinataire, ouvre un registre spécial où sont enregistrés dès réception les documents classifiés communiqués par l'UE. Le registre est divisé en colonnes indiquant la date de réception du document, ses références (cote, date, numéro d'exemplaire), sa classification, son objet, le nom ou la fonction du destinataire, la date de renvoi du reçu à l'UE et la date de sa destruction.

14. *Utilisation et protection des informations classifiées échangées*

a) Les informations du degré SECRET UE sont traitées par des agents expressément désignés à cet effet et autorisés à avoir accès à des informations de ce degré de classification. Elles sont conservées dans des armoires de sécurité de bonne qualité qui ne peuvent être ouvertes que par des personnes autorisées à avoir accès aux informations qu'elles contiennent. Les zones dans lesquelles se trouvent ces armoires doivent être gardées en permanence et un système de contrôle doit être mis en place afin de n'y laisser entrer que les personnes dûment autorisées. Les informations du degré SECRET UE sont transmises par courrier diplomatique, services de messagerie protégée et moyens de télécommunications protégées. Des copies d'un document du degré SECRET UE ne peuvent être faites qu'avec l'accord écrit de l'autorité d'origine. Toutes les copies sont enregistrées et contrôlées. Des reçus doivent être délivrés pour toutes les opérations concernant les documents du degré SECRET UE.

b) Les informations du degré CONFIDENTIEL UE sont traitées par des agents dûment désignés et autorisés à être informés de la question traitée. Les documents sont conservés dans des armoires de sécurité verrouillés se trouvant dans des zones contrôlées.

Les informations du degré CONFIDENTIEL UE sont transmises par courrier diplomatique ou service de messagerie militaire et par des moyens de télécommunications protégées. Des copies peuvent en être faites par l'organisme destinataire; leur nombre et leur diffusion sont indiqués sur des registres spéciaux.

c) Les informations du degré RESTREINT UE sont traitées dans des locaux inaccessibles aux personnes non autorisées et sont conservées dans des meubles verrouillés. Les documents peuvent être transmis par les services postaux publics en tant qu'envois recommandés sous double enveloppe et, en cas d'urgence, par le réseau de télécommunications public. Des copies peuvent être faites par les destinataires.

d) Les informations sans classification ne nécessitent pas de mesures de protection particulières et peuvent être transmises par les services postaux et réseaux de télécommunications publics. Des copies peuvent en être faites par les destinataires.

15. *Destruction*

Les documents qui ne sont plus nécessaires doivent être détruits. Pour les documents des degrés RESTREINT UE et CONFIDENTIEL UE, une mention appropriée est indiquée dans les registres spéciaux. Pour les documents du degré SECRET UE, des procès-verbaux de destruction, signés par deux personnes ayant été témoins de l'opération, sont établis.

16. *Infractions à la sécurité*

Lorsque l'on constate ou que l'on soupçonne la compromission d'informations des degrés CONFIDENTIEL UE ou SECRET UE, l'ANS de l'État ou le responsable de la sécurité de l'organisation effectue une enquête sur les circonstances de la compromission. Si celle-ci est confirmée par l'enquête, l'autorité qui est à l'origine du document est informée. Les mesures nécessaires sont prises pour remédier à des procédures ou à un mode de conservation inadaptés s'ils sont à l'origine de la compromission. Le Secrétaire général du Conseil/Haut représentant ou l'ANS de l'État membre qui a communiqué les informations compromises peuvent demander au bénéficiaire des précisions concernant l'enquête.