Ce document constitue un outil de documentation et n'engage pas la responsabilité des institutions

►**B**

DÉCISION DE LA COMMISSION

du 29 novembre 2001

modifiant son règlement intérieur

[notifiée sous le numéro C(2001) 3031]

(2001/844/CE, CECA, Euratom)

(JO L 317 du 3.12.2001, p. 1)

Modifiée par:

		Journal officiel		
		n°	page	date
►**M1**	Décision 2005/94/CE, Euratom de la Commission du 3 février 2005	L 31	66	4.2.2005
►**M2**	Décision 2006/70/CE, Euratom de la Commission du 31 janvier 2006	L 34	32	7.2.2006
►**M3**	Décision 2006/548/CE, Euratom de la Commission du 2 août 2006	L 215	38	5.8.2006
►**M4**	Règlement (UE) nº 519/2013 de la Commission du 21 février 2013	L 158	74	10.6.2013

Rectifiée par:

►**C1** Rectificatif, JO L 37 du 10.2.2005, p. 21 (2001/844/CE, CECA, Euratom)

▼B

DÉCISION DE LA COMMISSION

du 29 novembre 2001

modifiant son règlement intérieur

[notifiée sous le numéro C(2001) 3031]

(2001/844/CE, CECA, Euratom)

LA COMMISSION DES COMMUNAUTÉS EUROPÉENNES,

vu le traité instituant la Communauté européenne, et notamment son article 218, paragraphe 2,

vu le traité instituant la Communauté européenne du charbon et de l'acier, et notamment son article 16,

vu le traité instituant la Communauté européenne de l'énergie atomique, et notamment son article 131,

vu le traité sur l'Union européenne, et notamment son article 28, paragraphe 1, et son article 41, paragraphe 1,

DÉCIDE:

Article premier

Les dispositions de la Commission en matière de sécurité, dont le texte figure à l'annexe de la présente décision, sont ajoutées en annexe au règlement intérieur de la Commission.

Article 2

La présente décision entre en vigueur le jour de sa publication au *Journal officiel des Communautés européennes*.

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

▼B

ANNEXE

DISPOSITIONS DE LA COMMISSION EN MATIÈRE DE SÉCURITÉ

Considérant ce qui suit:

(1) Afin de développer les activités de la Commission dans des domaines qui requièrent un certain degré de confidentialité, il convient de mettre en place un système de sécurité global applicable à la Commission, aux autres institutions, aux instances, bureaux et agences établis en vertu ou sur la base du traité CE ou du traité sur l'Union européenne, aux États membres ainsi qu'à tout autre destinataire d'informations classifiées de l'Union européenne, ci-après dénommées «informations classifiées de l'UE».

(2) Afin d'assurer l'efficacité du système de sécurité ainsi créé, la Commission limitera la communication d'informations classifiées de l'UE aux seuls organismes extérieurs qui offrent des garanties démontrant qu'ils ont pris toutes les mesures nécessaires à l'application de règles strictement équivalentes à celles des présentes dispositions.

(3) Les présentes dispositions sont arrêtées sans préjudice du règlement n° 3 du Conseil de la CEEA du 31 juillet 1958 portant application de l'article 24 du traité instituant la Communauté européenne de l'énergie atomique [1], du règlement (Euratom, CEE) n° 1588/90 du Conseil du 11 juin 1990 relatif à la transmission à l'Office statistique des Communautés européennes d'informations statistiques couvertes par le secret [2] ni de la décision C(95) 1510 final de la Commission du 23 novembre 1995 relative à la protection des systèmes d'information.

(4) Afin d'assurer le bon fonctionnement du processus de décision au sein de l'Union, la Commission élabore son système de sécurité sur la base des principes énoncés dans la décision 2001/264/CE du Conseil du 19 mars 2001 adoptant le règlement de sécurité du Conseil [3].

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

(6) La Commission reconnaît la nécessité de créer son propre concept de sécurité, en tenant compte de tous les éléments relatifs à la sécurité et du caractère spécifique de la Commission en tant qu'institution.

(7) Les présentes dispositions sont arrêtées sans préjudice de l'article 255 du traité, ni du règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission [4].

▼M2

(8) Les présentes dispositions sont sans préjudice de l'article 286 du traité, ni du règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données,

▼B

Article premier

Les règles en matière de sécurité figurent à l'annexe.

---

[1] JO n° 17 du 6.10.1958, p. 406/58.
[2] JO L 151 du 15.6.1990, p. 1.
[3] JO L 101 du 11.4.2001, p. 1.
[4] JO L 145 du 31.5.2001, p. 43.

▼B

Article 2

1. Le membre de la Commission chargé des questions de sécurité prend les mesures appropriées pour faire en sorte que, lors du traitement d'informations classifiées de l'UE, les règles visées à l'article 1er soient respectées au sein de la Commission par ses fonctionnaires et autres agents comme par le personnel détaché auprès de la Commission, ainsi que dans tous les lieux de travail de la Commission, y compris ses représentations et bureaux dans l'Union et ses délégations dans les pays tiers, et également par les contractants extérieurs de la Commission.

▼M3

Lorsqu'un contrat ou une convention de subvention entre la Commission et un contractant extérieur ou un bénéficiaire implique le traitement d'informations classifiées de l'UE dans les locaux du contractant ou du bénéficiaire, les mesures appropriées devant être prises par ledit contractant extérieur ou par ledit bénéficiaire afin de veiller au respect, lors du traitement des informations classifiées de l'UE, les règles visées à l'article 1er font partie intégrante du contrat ou de la convention de subvention.

▼B

2. Les États membres, les autres institutions ainsi que les instances, bureaux et agences établis en vertu ou sur la base des traités pourront recevoir des informations classifiées de l'UE pourvu qu'ils veillent à ce que des règles strictement équivalentes à celles visées à l'article 1er soient appliquées, dans leurs services et leurs locaux, au traitement de telles informations, notamment 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 de la Commission ou de ses instances, ou participant à d'autres activités de la Commission;

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 et le personnel détaché qui traitent des informations classifiées de l'UE.

Article 3

Les pays tiers, organisations internationales et autres organismes pourront recevoir des informations classifiées de l'UE pourvu qu'ils assurent, dans le traitement de ces informations, le respect de règles strictement équivalentes à celles visées à l'article 1er.

Article 4

Dans le respect des principes de base et des normes minimales de sécurité figurant dans la partie I de l'annexe, le membre de la Commission chargé des questions de sécurité peut prendre des mesures conformément à la partie II de l'annexe.

Article 5

À compter de leur date d'application, les présentes dispositions remplacent:

a) la décision C(94) 3282 de la Commission du 30 novembre 1994 relative aux mesures de sécurité applicables aux informations classifiées produites ou transmises dans le cadre des activités de l'Union européenne;

b) la décision C(1999) 423 de la Commission du 25 février 1999 relative aux modalités selon lesquelles les fonctionnaires et agents de la Commission européenne peuvent être autorisés à avoir accès à des informations classifiées détenues par la Commission.

▼B

Article 6

À compter de la date d'application des présentes dispositions, toutes les informations classifiées détenues par la Commission jusqu'à cette date, à l'exception des informations classées Euratom sont:

a) lorsqu'elles ont été créées par la Commission, considérées comme reclassifiées par défaut dans la catégorie «RESTREINT UE», à moins que leur auteur ne décide de leur attribuer une autre classification au plus tard le 31 janvier 2002. Dans ce dernier cas, l'auteur informe tous les destinataires du document concerné;

b) lorsqu'elles ont été créées par des personnes extérieures à la Commission, maintenues dans leur classification originelle et donc traitées comme des informations classifiées de l'UE du même niveau, à moins que l'auteur n'accepte de les déclassifier ou de les déclasser.

▼B

ANNEXE

RÈGLES EN MATIÈRE DE SÉCURITÉ

Sommaire

PARTIE I: PRINCIPES DE BASE ET NORMES MINIMALES DE SÉCURITÉ

1. INTRODUCTION

2. PRINCIPES GÉNÉRAUX

3. FONDEMENTS D'UNE BONNE SÉCURITÉ

4. PRINCIPES RELATIFS À LA SÉCURITÉ DES DONNÉES

4.1. **Objectifs**

4.2. **Définitions**

4.3. **Classification**

4.4. **Objectifs des mesures de sécurité**

5. ORGANISATION DE LA SÉCURITÉ

5.1. **Normes minimales communes**

5.2. **Organisation**

6. MESURES DE SÉCURITÉ RELATIVES AU PERSONNEL

6.1. **Habilitations de sécurité**

6.2. **Registres des habilitations de sécurité du personnel**

6.3. **Formation du personnel dans le domaine de la sécurité**

6.4. **Responsabilités du personnel d'encadrement**

6.5. **Statut du personnel en matière de sécurité**

7. SÉCURITÉ PHYSIQUE

7.1. **Exigences en matière de protection**

7.2. **Contrôles**

7.3. **Sécurité des bâtiments**

7.4. **Plans d'urgence**

8. SÉCURITÉ DES INFORMATIONS

9. PROTECTION CONTRE LE SABOTAGE OU TOUT AUTRE ACTE INTENTIONNEL DE DÉTÉRIORATION

10. COMMUNICATIONS D'INFORMATIONS CLASSIFIÉES À DES PAYS TIERS OU À DES ORGANISATIONS INTERNATIONALES

PARTIE II:ORGANISATION DE LA SÉCURITÉ AU SEIN DE LA COMMISSION

11. LE MEMBRE DE LA COMMISSION CHARGÉ DES QUESTIONS DE SÉCURITÉ

12. LE GROUPE CONSULTATIF DE LA COMMISSION SUR LA POLITIQUE DE SÉCURITÉ

13. LE COMITÉ DE SÉCURITÉ DE LA COMMISSION

14. LA ►**M2** DIRECTION DE LA SÉCURITÉ DE LA COMMISSION ◄

15. INSPECTIONS DE SÉCURITÉ

16. CLASSIFICATIONS; TIMBRES ET IDENTIFIANTS DE SÉCURITÉ

16.1. **Degrés de classification**

▼B

16.2. **Identifiants de sécurité**

16.3. **Timbres**

16.4. **Apposition de la classification**

16.5. **Apposition des identifiants de sécurité**

17. POLITIQUE EN MATIÈRE DE CLASSIFICATION

17.1. **Généralités**

17.2. **Détermination de la classification**

17.3. **Déclassement et déclassification**

18. SÉCURITÉ PHYSIQUE

18.1. **Généralités**

18.2. **Exigences de sécurité**

18.3. **Mesures physiques de sécurité**

18.3.1. *Zones de sécurité*

18.3.2. *Zone administrative*

18.3.3. *Contrôle des entrées et des sorties*

18.3.4. *Rondes*

18.3.5. *Meubles de sécurité et chambres fortes*

18.3.6. *Serrures*

18.3.7. *Contrôle des clés et combinaisons*

18.3.8. *Dispositifs de détection des intrusions*

18.3.9. *Matériels agréés*

18.3.10. *Protection physique des photocopieuses et des télécopieurs*

18.4. **Protection contre la néglicence et les écoutes clandestines**

18.4.1. *Protection contre les regards*

18.4.2. *Protection contre les écoutes*

18.4.3. *Introduction d'appareils électroniques et de matériel d'enregistrement*

18.5. **Zones protégées sur le plan technique**

19. RÈGLES GÉNÉRALES RELATIVES AU BESOIN D'EN CONNAÎTRE ET AUX HABILITATIONS DE SÉCURITÉ DU PERSONNEL DE L'UE

19.1. **Généralités**

19.2. **Règles spécifiques concernant l'accès aux informations classifiées TRES SECRET UE/EU TOP SECRET**

19.3. **Règles spécifiques concernant l'accès aux informations classifiées TRES SECRET UE/EU TOP SECRET et CONFIDENTIEL UE**

19.4. **Règles spécifiques concernant l'accès aux informations classifiées RESTREINT UE**

19.5. **Mutations**

19.6. **Instructions spéciales**

▼B

20. PROCÉDURE D'HABILITATION DE SÉCURITÉ POUR LES FONCTIONNAIRES ET AUTRES AGENTS DE LA COMMISSION

21. PRÉPARATION, RÉPARTITION, TRANSMISSION, MESURES DE SÉCURITÉ RELATIVES AUX COURRIERS, EXEMPLAIRES SUPPLÉMENTAIRES, TRADUCTIONS ET EXTRAITS DE DOCUMENTS CLASSIFIÉS DE L'UE

21.1. **Préparation**

21.2. **Diffusion**

21.3. **Transmission/transport de documents classifiés de l'UE**

21.3.1. *Emballages et récépissés*

21.3.2. *Transmission au sein d'un bâtiment ou d'un groupe de bâtiments*

21.3.3. *Transmission à l'intérieur d'un même pays*

21.3.4. *Transmission d'un État à un autre*

21.3.5. *Transmission/transport de documents classifiés de l'UE*

21.4. **Mesures de sécurité relatives aux courriers**

21.5. **Transmission par voie électronique ou d'autres moyens techniques**

21.6. **Exemplaires supplémentaires et traductions et extraits de documents classifiés de l'UE**

22. BUREAUX D'ORDRE, REGROUPEMENTS, CONTRÔLES, ARCHIVAGE ET DESTRUCTION DE DOCUMENTS CLASSIFIÉS DE L'UE

22.1. **Bureaux d'ordre locaux chargés des documents classifiés de l'UE**

22.2. **Le bureau d'ordre TRES SECRET UE/EU TOP SECRET**

22.2.1. *Généralités*

22.2.2. *Le bureau d'ordre central TRES SECRET UE/EU TOP SECRET*

22.2.3. *Bureaux d'ordre TRES SECRET UE/EU TOP SECRET subordonnés*

22.3. **Inventaires, regroupements et contrôles de documents classifiés de l'UE**

22.4. **Archivage d'informations classifiées de l'UE**

22.5. **Destruction des documents classifiés de l'UE**

22.6. **Destruction en cas d'urgence**

23. MESURES DE SÉCURITÉ À APPLIQUER À L'OCCASION DES RÉUNIONS SPÉCIFIQUES TENUES EN DEHORS DES LOCAUX DE LA COMMISSION ET METTANT EN JEU DES INFORMATIONS CLASSIFIÉES DE L'UE

23.1. **Généralités**

23.2. **Les responsabilités**

23.2.1. *La* ►**M2** *direction de la sécurité de la Commission* ◄

23.2.2. *Le responsable de la sécurité de la réunion*

23.3 **Mesures de sécurité**

23.3.1. *Zones de sécurité*

23.3.2. *Laissez-passer*

23.3.3. *Contrôle des appareils photographiques et des appareils d'enregistrement*

▼B

23.3.4. *Contrôle des porte-documents, ordinateurs portatifs et paquets*

23.3.5. *Sécurité technique*

23.3.6. *Documents des délégations*

23.3.7. *Conservation des documents en lieu sûr*

23.3.8. *Vérification des bureaux*

23.3.9. *Élimination des rebuts classifiés de l'UE*

24. INFRACTIONS À LA SÉCURITÉ ET COMPROMISSION DES INFORMATIONS CLASSIFIÉES DE L'UE

24.1. **Définitions**

24.2. **Dénonciation des infractions à la sécurité**

24.3. **Actions en justice**

25. PROTECTION DES INFORMATIONS CLASSIFIÉES DE L'UE TRANSITANT PAR DES SYSTÈMES DE COMMUNICATION ET D'INFORMATION

25.1. **Introduction**

25.1.1. *Généralités*

25.1.2. *Vulnérabilité des systèmes et menaces éventuelles*

25.1.3. *But principal des mesures de sécurité*

25.1.4. *Énoncé des impératifs de sécurité propres à un système (SSRS)*

25.1.5. *Modes d'exploitation de sécurité*

25.2. **Définitions**

25.3. **Responsabilités en matière de sécurité**

25.3.1. *Généralités*

25.3.2. *L'autorité d'homologation de sécurité (SAA)*

25.3.3. *L'autorité INFOSEC (IA)*

25.3.4. *Le propriétaire des systèmes techniques (TSO)*

25.3.5. *Le propriétaire de l'information (IO)*

25.3.6. *Utilisateurs*

25.3.7. *Formation INFOSEC*

25.4. **Mesures de sécurité non techniques**

25.4.1. *Sécurité du personnel*

25.4.2. *Sécurité physique*

25.4.3. *Contrôle des accès à un système*

25.5. **Mesures de sécurité techniques**

25.5.1. *Sécurité des informations*

25.5.2. *Contrôle et comptabilisation des informations*

25.5.3. *Manipulation et contrôle des supports amovibles*

▼B

25.5.4. *Déclassification et destruction des supports informatiques*

25.5.5. *Sécurité des communications*

25.5.6. *Mesures de sécurité concernant l'installation et le rayonnement*

25.6. **Sécurité pendant le traitement**

25.6.1. *Procédures d'exploitation de sécurité (SecOP)*

25.6.2. *Protection et gestion de la configuration des logiciels*

25.6.3. *Détection de la présence de logiciels malveillants ou de virus informatiques*

25.6.4. *Maintenance*

25.7. **Acquisition**

25.7.1. *Généralités*

25.7.2. *Homologation*

25.7.3. *Évaluation et certification*

25.7.4. *Contrôle systématique des dispositifs de sécurité pour la prorogation de l'homologation*

25.8. **Utilisation temporaire ou occasionnelle**

25.8.1. *Sécurité des micro-ordinateurs et ordinateurs individuels*

25.8.2. *Utilisation de matériel TI personnel pour un travail officiel dans le cadre de la Commission*

25.8.3. *Utilisation de matériel TI appartenant à un contractant ou fourni par un pays pour un travail officiel dans le cadre de la Commission*

26. COMMUNICATION D'INFORMATIONS CLASSIFIÉES DE L'UE À DES PAYS TIERS OU À DES ORGANISATIONS INTERNATIONALES

26.1.1. *Principes régissant la communication d'informations classifiées de l'UE*

26.1.2. *Les niveaux*

26.1.3. *Accords de sécurité*

Appendice 1: **Tableau comparatif des classifications de sécurité nationales**

Appendice 2: **Guide pratique de la classification**

Appendice 3: **Lignes directrices concernant la communication d'informations classifiées de l'UE à des États tiers ou à des organisations internationales Niveau 1 de coopération**

Appendice 4: **Lignes directrices concernant la communication d'informations classifiées de l'UE à des États tiers ou à des organisations internationales Niveau 2 de coopération**

Appendice 5: **Lignes directrices concernant la communication d'informations classifiées de l'UE à des États tiers ou à des organisations internationales Niveau 3 de coopération**

Appendice 6: **Liste des abréviations**

▼B

PARTIE I: PRINCIPES DE BASE ET NORMES MINIMALES DE SÉCURITÉ

1. INTRODUCTION

Les présentes règles définissent les principes de base et les normes minimales de sécurité à observer comme il convient par la Commission dans tous ses lieux de travail ainsi que par tout destinataire d'informations classifiées de l'UE, de manière à assurer la sécurité et de sorte que chacun puisse avoir la certitude qu'une norme de protection commune est établie.

2. PRINCIPES GÉNÉRAUX

La politique de sécurité de la Commission fait partie intégrante de sa politique de gestion interne générale et est par conséquent basée sur les principes régissant sa politique générale.

Ces principes comprennent la légalité, la transparence, la responsabilité et la subsidiarité (proportionnalité).

Par légalité on entend la nécessité de maintenir strictement dans le cadre juridique l'exécution des fonctions de sécurité, ainsi que la nécessité de se conformer aux exigences légales. Les dispositions du statut des fonctionnaires et autres agents s'appliquent pleinement, en particulier son article 17 concernant l'obligation de discrétion à l'égard des informations de la Commission et son titre VI concernant les mesures disciplinaires. Ce concept implique également que les responsabilités en matière de sécurité doivent s'appuyer sur des dispositions juridiques appropriées. Enfin, il implique que les manquements aux règles de sécurité commis dans les domaines de responsabilité de la Commission doivent être traités conformément à la politique de la Commission en matière d'actions disciplinaires et à sa politique de coopération avec les États membres dans le domaine de la justice pénale.

Par «transparence» on entend la nécessité d'établir des règles et dispositions de sécurité universellement caractérisées par leur clarté et d'assurer l'équilibre entre les différents services et les différents domaines (sécurité physique par opposition à protection des données, etc.) ainsi que la nécessité d'une politique cohérente et structurée de sensibilisation à la sécurité. Ce concept implique également la nécessité de disposer d'orientations écrites claires pour la mise en œuvre des mesures de sécurité.

Par responsabilité, on entend la nécessité non seulement de définir clairement les responsabilités dans le domaine de la sécurité, mais également de contrôler régulièrement si ces responsabilités ont été correctement exécutées.

Par subsidiarité, ou proportionnalité, on entend que la sécurité doit être organisée dès le plus bas niveau possible et au plus près des directions générales et des services de la Commission. Ce concept implique également la nécessité de limiter les actions de sécurité aux éléments pour lesquelles elles se justifient véritablement. Il signifie enfin que les mesures de sécurité doivent être proportionnelles aux intérêts à protéger et aux menaces réelles ou potentielles qui pèsent sur ces intérêts, de manière à en organiser la protection dans des conditions imposant le moins de perturbations possible.

3. FONDEMENTS D'UNE BONNE SÉCURITÉ

Un système de sécurité fiable a pour fondements:

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

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

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

▼B

b) au sein de chaque État membre et au sein de la Commission, une autorité technique INFOSEC (IA) 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 gouvernementaux et les services compétents de la Commission, pour déterminer et recommander, selon ce qui convient:

1) les personnes, informations les ressources à protéger;

2) les normes communes de protection.

d) une étroite collaboration entre, d'une part, la ►M2 direction de la sécurité de la Commission ◄ et, d'autre part, les services de sécurité des autres institutions européennes et le bureau de sécurité de l'OTAN (NOS).

4. PRINCIPES RELATIFS À LA SÉCURITÉ DES DONNÉES

4.1. **Objectifs**

La sécurité des données 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 confidentialité, leur intégrité et leur disponibilité;

c) la sauvegarde des locaux de la Commission 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 des mesures correctives nécessaires.

4.2. **Définitions**

Aux fins des présentes règles, on entend par:

a) «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;

b) «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;

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

d) «besoin d'en connaître» la nécessité, pour un employé, d'accéder à des informations classifiées de l'UE pour pouvoir s'acquitter d'une fonction ou d'une tâche donnée;

e) «autorisation» une décision par laquelle le ►M2 directeur de la direction de la sécurité de la Commission ◄ permet à un individu d'accéder à des informations classifiées de l'UE jusqu'à un niveau donné, sur la base du résultat positif d'une enquête de sécurité (procédure d'habilitation) effectuée par une autorité nationale de sécurité conforme au droit national;

▼B

f) «classification» l'attribution d'un niveau de sécurité approprié à une information dont la divulgation non autorisée serait susceptible de causer un certain préjudice aux intérêts de la Commission ou de ses États membres;

g) «déclassement» («downgrading»), une diminution du degré de la classification;

h) «déclassification» («declassification») la suppression de toute mention de classification;

i) «autorité d'origine» l'auteur, dûment autorisé, d'un document classifié; à la Commission, les chefs de service peuvent autoriser leur personnel à délivrer une classification.

j) «services de la Commission» les unités et services de la Commission, dont les cabinets, dans tous les lieux de travail, y compris le Centre commun de recherche, les représentations et bureaux de la Commission dans l'Union et les délégations dans les pays tiers.

4.3. **Classification**

a) 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 tant la surclassification que la sous-classification.

b) Le système de classification constitue l'instrument qui permet de mettre en œuvre ces principes; il convient 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.

c) L'autorité d'origine de l'information est seule responsable de sa classification.

d) La détermination du degré de classification se fonde exclusivement sur le contenu de l'information concernée.

e) Lorsqu'un certain nombre de renseignements sont regroupés, le degré de classification appliqué à l'ensemble est au moins égal au degré le plus élevé de classification des parties. On peut néanmoins attribuer à un groupement d'informations une classification plus élevée que celle de ses composantes.

f) Les classifications sont attribuées uniquement en cas de nécessité et maintenues aussi longtemps que nécessaire.

4.4. **Objectifs des mesures de sécurité**

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;

▼B

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.

5. ORGANISATION DE LA SÉCURITÉ

5.1. **Normes minimales communes**

La Commission veille à ce que les normes minimales communes en matière de sécurité soient observées par tout destinataire d'une information classifiée de l'UE, interne et relevant de sa compétence, comme par exemple les services et les contractants de la Commission, de sorte que l'on ait la certitude que toute information classifiée de l'UE sera traitée par tous 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.

L'accès à des informations classifiées de l'UE ne peut être autorisé par la Commission à des organismes extérieurs que pour autant qu'ils observent, dans la manipulation de telles informations, des dispositions qui soient au moins strictement équivalentes aux présentes normes minimales.

▼M3

Ces normes minimales sont également appliquées lorsque la Commission confie, par voie de contrat ou de convention de subvention, à des entités industrielles ou autres, des tâches qui font intervenir, nécessitent et/ou comportent des informations classifiées de l'UE: ces normes minimales communes sont énoncées à la partie II, section 27.

▼B

5.2. **Organisation**

Au sein de la Commission, la sécurité est organisée à deux niveaux:

a) à l'échelle de la Commission dans son ensemble, il existe une ►M2 direction de la sécurité de la Commission ◄ associée à une autorité d'homologation de sécurité (SAA) qui joue également le rôle d'autorité Crypto (CrA) et d'autorité TEMPEST, à une autorité INFOSEC (IA) ainsi qu'à un ou plusieurs bureaux d'ordre centraux pour les informations classifiées de l'UE comptant chacun un ou plusieurs agents contrôleurs (RCO).

b) au niveau des services de la Commission, la sécurité est confiée à un ou plusieurs responsables locaux de sécurité (LSO), un ou plusieurs responsables centraux de la sécurité informatique (CISO), des responsables locaux de la sécurité informatique et des bureaux d'ordre locaux pour les informations classifiées de l'UE comptant chacun un ou plusieurs agents contrôleurs.

c) Les organes centraux de sécurité fournissent aux organes locaux des instructions opérationnelles.

6. MESURES DE SÉCURITÉ RELATIVES AU PERSONNEL

6.1. **Habilitations de sécurité**

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

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.

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 ►**M1** SECRET UE ◄;

f) auxquelles leurs fonctions confèrent un accès spécial aux systèmes de communication ou d'information protégés 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.

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.

6.2. **Registres des habilitations de sécurité du personnel**

Tout service de la Commission ayant à traiter des informations classifiées de l'UE ou hébergeant des systèmes de communication ou d'information protégés doit tenir un registre des habilitations accordées à cet effet 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 responsable local de sécurité du service de la Commission tient le registre des habilitations du domaine placé sous son contrôle.

6.3. **Formation du personnel dans le domaine de la sécurité**

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 obligatoire que tous ces membres du personnel certifient par écrit avoir pleinement compris les règles de sécurité applicables à leur poste.

6.4. **Responsabilités du personnel d'encadrement**

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 protégés, de prendre note des incidents ou vulnérabilités manifestes pouvant avoir des répercussions sur le plan de la sécurité, et de les signaler.

6.5. **Statut du personnel en matière de sécurité**

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 protégés, et d'informer la ►**M2** direction de la sécurité de la Commission ◄. 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.

▼B

7. SÉCURITÉ PHYSIQUE

7.1. **Exigences en matière de protection**

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. 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.

7.2. **Contrôles**

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.

7.3. **Sécurité des bâtiments**

Les bâtiments contenant des informations classifiées de l'UE ou des systèmes de communication et d'information protégés doivent être défendus contre l'accès des personnes non autorisées. La nature de cette défense (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.

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.

7.4. **Plans d'urgence**

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.

8. SÉCURITÉ DES INFORMATIONS

La sécurité des informations (INFOSEC) a trait à la détermination et à l'application des mesures de sécurité permettant de protéger les informations classifiées de l'UE 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 à des informations classifiées de l'UE et que des utilisateurs autorisés se voient refuser l'accès à ces informations, et afin d'en empêcher l'altération, la modification ou la destruction non autorisées.

▼B

9. PROTECTION CONTRE LE SABOTAGE OU TOUT AUTRE ACTE INTENTIONNEL DE DÉTÉRIORATION

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 fournir les renseignements ayant trait à des activités d'espionnage, de sabotage, de terrorisme et à d'autres activités subversives.

10. COMMUNICATION D'INFORMATIONS CLASSIFIÉES À DES PAYS TIERS OU À DES ORGANISATIONS INTERNATIONALES

Il appartient au collège des membres de la Commission d'autoriser la communication à un État tiers ou à une organisation internationale d'informations classifiées de l'UE émanant de la Commission. Si l'autorité d'origine des informations à communiquer n'est pas la Commission, celle-ci doit au préalable lui demander son consentement. Au cas où l'autorité d'origine ne peut être identifié, la Commission en assume la responsabilité.

Si la Commission reçoit des informations classifiées de pays tiers, d'organisations internationales ou d'autres tiers, celles-ci reçoivent une protection conforme à leur classification et correspondant aux normes établies dans les présentes dispositions relatives aux informations classifiées de l'UE, ou correspondant aux normes plus strictes qui pourraient être exigées par le tiers qui communique ces informations. Des contrôles réciproques peuvent être prévus.

Les principes susmentionnés sont appliqués conformément aux dispositions détaillées figurant dans la partie II, section 26, et dans les appendices 3, 4 et 5.

PARTIE II: ORGANISATION DE LA SÉCURITÉ AU SEIN DE LA COMMISSION

11. LE MEMBRE DE LA COMMISSION CHARGÉ DES QUESTIONS DE SÉCURITÉ

Le membre de la Commission chargé des questions de sécurité:

a) applique la politique de sécurité de la Commission;

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

c) examine les questions impliquant des changements dans la politique de sécurité de la Commission, en étroite liaison avec les autorités nationales de sécurité (ou autres autorités appropriées) des États membres (ci-après dénommées «ANS»).

Le membre de la Commission chargé des questions de sécurité est notamment responsable:

a) de coordonner toutes les questions de sécurité liées aux activités de la Commission;

b) de demander aux ANS des États membres de fournir les habilitations de sécurité intéressant le personnel employé au SGC conformément à la section 20;

c) d'enquêter ou d'ordonner une enquête sur toute fuite concernant les informations classifiées de l'UE qui, d'après les premiers indices, se serait produite à partir de la Commission;

d) de demander aux autorités de sécurité compétentes d'ouvrir une enquête lorsqu'une fuite concernant des informations classifiées de l'UE semble s'être produite en dehors de la Commission et de coordonner les enquêtes lorsqu'elles impliquent plus d'une autorité de sécurité;

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

▼B

f) de rester en liaison étroite avec toutes les autorités de sécurité concernées dans l'intérêt d'une coordination globale de la sécurité;

g) de réexaminer constamment l'organisation et les procédures de sécurité de la Commission et, le cas échéant, de préparer les recommandations qui s'imposent. À cet égard, le membre de la Commission chargé des questions de sécurité présente à la Commission le plan annuel d'inspection préparé par la ►M2 direction de la sécurité de la Commission ◄.

12. LE GROUPE CONSULTATIF DE LA COMMISSION SUR LA POLITIQUE DE SÉCURITÉ

Un groupe consultatif sur la politique de sécurité est établi au sein de la Commission. Celui-ci est constitué des représentants des autorités nationales de sécurité de chaque État membre et présidé par le membre de la Commission chargé des questions de sécurité ou son adjoint. Les représentants d'autres institutions européennes peuvent être également invités. Des représentants des organismes décentralisés de la CE et de l'UE peuvent également être invités à assister à ses réunions lorsque les questions traitées les concernent.

Le groupe consultatif sur la politique de sécurité se réunit à la demande de son président ou de n'importe lequel de ses membres. Il a pour tâche d'examiner et d'évaluer toutes les questions pertinentes en matière de sécurité et de présenter le cas échéant des recommandations à la Commission.

▼M2

13. LE COMITÉ DE SÉCURITÉ DE LA COMMISSION

Un comité de sécurité est établi au sein de la Commission. Présidé par le directeur général de la direction générale Personnel et administration, il réunit un membre du cabinet du commissaire chargé des questions de sécurité, un membre du cabinet du président, le secrétaire général adjoint, qui préside le groupe de gestion des crises de la Commission, les directeurs généraux du service juridique, de la direction générale Relations extérieures, de la direction générale Justice, liberté et sécurité, du Centre commun de recherche, de la direction générale Informatique et du service d'audit interne, ainsi que le directeur de la direction de la sécurité de la Commission, ou leurs représentants. D'autres fonctionnaires de la Commission peuvent être invités. Ce comité a pour mandat d'évaluer les mesures de sécurité au sein de la Commission et d'adresser des recommandations en la matière au membre de la Commission chargé des questions de sécurité.

▼B

14. LA ►M2 DIRECTION DE LA SÉCURITÉ DE LA COMMISSION ◄

Pour s'acquitter des tâches qui lui incombent en vertu de la section 11, le membre de la Commission chargé des questions de sécurité est assisté de la ►M2 direction de la sécurité de la Commission ◄ pour ce qui concerne la coordination, la supervision et l'application des mesures de sécurité.

Le ►M2 directeur de la direction de la sécurité de la Commission ◄ est le conseiller principal, en matière de sécurité, du membre de la Commission chargé des questions de sécurité. Il est également secrétaire du groupe consultatif sur la politique de sécurité. À ce titre, il dirige les travaux d'actualisation de la réglementation de sécurité et assure la coordination des mesures de sécurité avec les autorités compétentes des États membres et, le cas échéant, avec les organisations internationales liées à la Commission par des accords de sécurité. À cette fin, il joue le rôle d'officier de liaison.

Le ►M2 directeur de la direction de la sécurité de la Commission ◄ est responsable de l'homologation des systèmes et réseaux TI au sein de la commission. Il prend, en accord avec l'ANS compétente, les décisions relatives à l'homologation des systèmes et réseaux TI impliquant d'une part la Commission et d'autre part tout autre destinataire d'informations classifiées de l'UE.

▼B

15. INSPECTIONS DE SÉCURITÉ

La ►M2 direction de la sécurité de la Commission ◄ mène périodiquement des inspections relatives aux dispositions de sécurité prises pour assurer la protection des informations classifiées de l'UE.

Elle peut être assistée dans cette tâche par les services de sécurité d'autres institutions détentrices d'informations classifiées de l'UE ou par les autorités de sécurité nationales des États membres ([1]).

Tout État membre peut, sur demande, faire réaliser par son ANS une inspection des dispositions de protection des informations classifiées de l'UE au sein de la Commission; cette inspection est réalisée conjointement et en commun accord avec la ►M2 direction de la sécurité de la Commission ◄.

16. CLASSIFICATIONS; TIMBRES ET IDENTIFIANTS DE SÉCURITÉ

16.1. **Degrés de classification** ([2])

Les informations sont classifiées selon les degrés dont la liste suit (cf. appendice 2):

►M1 TRES SECRET UE/EU TOP SECRET ◄: 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 plusieurs de ses États membres.

SECRET UE: 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 plusieurs de ses États membres.

CONFIDENTIEL UE: 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.

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

Aucune autre classification n'est permise.

16.2. **Identifiants de sécurité**

Pour fixer des limites à la validité d'une classification (c'est-à-dire le moment où l'information classifiée est automatiquement déclassée ou déclassifiée), il est possible d'utiliser un identifiant de sécurité convenu. Cet identifiant peut être «JUSQU'À/AU … (heure/date» ou «JUSQU'À/AU … (événement)».

Des identifiants complémentaires tels que CRYPTO ou tout autre identifiant reconnu 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.

Les identifiants de sécurité ne sont utilisés qu'en association avec une classification.

16.3. **Timbres**

Un timbre peut être utilisé pour préciser le domaine couvert par le document, pour indiquer une diffusion particulière fondée sur le besoin d'en connaître, ou (dans le cas d'une information non classifiée) pour indiquer la fin d'une interdiction.

Un timbre n'est pas une classification et ne saurait être utilisé en lieu et place d'une classification.

([1]) Sans préjudice de la convention de Vienne de 1961 sur les relations diplomatiques et le protocole sur les privilèges et immunités des Communautés européennes du 8 avril 1965.

([2]) Voir à l'annexe I un tableau comparatif des classifications de sécurité en usage dans l'UE, à l'OTAN, à l'UEO et dans les États membres.

▼B

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.

16.4. **Apposition de la classification**

La classification est apposée de la manière suivante:

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

b) sur les documents CONFIDENTIEL UE, par un procédé mécanique, à la main ou par impression sur du papier enregistré revêtu d'un cachet préimprimé;

c) sur les documents SECRET UE et ►M1 TRES SECRET UE/EU TOP SECRET ◄, par un procédé mécanique ou à la main.

16.5. **Apposition des identifiants de sécurité**

Les identifiants de sécurité sont apposés juste sous la classification, par les mêmes moyens que pour l'apposition des classifications.

17. POLITIQUE EN MATIÈRE DE CLASSIFICATION

17.1. **Généralités**

Les informations ne sont classifiées que si cela est nécessaire. La classification est clairement et correctement indiquée; elle est limitée à la durée pendant laquelle les informations doivent être protégées.

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

Les fonctionnaires et autres agents de la Commission classifient, déclassent ou déclassifient les informations sur instruction de leur chef de service ou en accord avec celui-ci.

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.

Le nombre de personnes autorisées à émettre des documents ►M1 TRES SECRET UE/EU TOP SECRET ◄ est limité au strict minimum. La liste nominative de ces personnes est conservée par la ►M2 direction de la sécurité de la Commission ◄.

17.2. **Détermination de la classification**

La classification d'un document est déterminée par le degré de sensibilité de son contenu, conformément aux définitions données à la section 16. Il importe que la classification soit utilisée à bon escient et avec modération. Cela s'applique particulièrement à la classification ►M1 TRES SECRET UE/EU TOP SECRET ◄.

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

Un guide pratique de la classification figure à l'appendice 2.

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

▼B

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.

L'accès public demeure régi par le règlement (CE) nº 1049/2001.

17.3. **Déclassement et déclassification**

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'autorité 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.

Dans la mesure du 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 demeure nécessaire.

18. SÉCURITÉ PHYSIQUE

18.1. **Généralités**

Les objectifs principaux 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, de faire obstacle au vol ou à la dégradation des équipements ou d'autres biens et de prévenir tout harcèlement ou autre type d'agression à l'encontre du personnel, d'autres employés ou des visiteurs.

18.2. **Exigences de sécurité**

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

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.

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;

c) empêcher à toute personne non motivée par le besoin d'en connaître d'accéder aux informations classifiées de l'UE.

▼B

18.3. **Mesures physiques de sécurité**

18.3.1. *Zones de sécurité*

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 services 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.

18.3.2. *Zone administrative*

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 ces zones administratives.

18.3.3. *Contrôle des entrées et des sorties*

À l'entrée et la sortie des zones de sécurité de catégorie I et II, toute personne travaillant ordinairement dans ces zones est contrôlée au moyen d'un système de laissez-passer ou d'identification individuelle. 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.

▼B

18.3.4. *Rondes*

En dehors des heures normales de travail, 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 toute compromission, détérioration ou perte. La fréquence de ces rondes est déterminée en fonction des conditions locales, mais elles doivent avoir lieu toutes les deux heures environ.

18.3.5. *Meubles de sécurité et chambres fortes*

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 ►**M1** TRES 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 uniquement.

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 SAA 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.

18.3.6. *Serrures*

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 uniquement.

18.3.7. *Contrôle des clés et combinaisons*

Les clés des meubles de sécurité ne doivent pas être emportées 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 local de la sécurité du service de la Commission concerné 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.

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, effective ou suspectée;

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

▼B

18.3.8. *Dispositifs de détection des intrusions*

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.

18.3.9. *Matériels agréés*

La ►M2 direction de la sécurité de la Commission ◄ tient à jour, par type et par modèle, les listes des matériels de sécurité qu'elle a agréés pour la protection directe ou indirecte des informations classifiées dans diverses circonstances et conditions qui auront été spécifiées. Pour l'établissement de ces listes, la ►M2 direction de la sécurité de la Commission ◄ se fonde, entre autres, sur les informations fournies par les ANS.

18.3.10. *Protection physique des photocopieuses et des télécopieurs*

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

18.4. **Protection contre la négligence et les écoutes clandestines**

18.4.1. *Protection contre les regards*

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.

18.4.2. *Protection contre les écoutes*

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

18.4.3. *Introduction d'appareils électroniques et de matériel d'enregistrement*

L'introduction de téléphones mobiles, d'ordinateurs privés, de dispositifs d'enregistrement, de caméras et d'autres dispositifs électroniques ou matériels d'enregistrements dans les secteurs de sécurité ou les zones protégées sur le plan technique n'est pas autorisée sans autorisation préalable du ►M2 directeur de la direction de la sécurité de la Commission ◄.

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), la ►M2 direction de la sécurité de la Commission ◄ peut demander l'aide des spécialistes des ANS.

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 ►M2 directeur de la direction de la sécurité de la Commission ◄, par des spécialistes de la sécurité technique des ANS.

▼B

18.5. **Zones protégées sur le plan technique**

Certaines zones peuvent être désignées comme zones protégées sur le plan technique. Un contrôle spécial doit être effectué à l'entrée. Ces zones 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, effective ou présumée, de personnel non autorisé.

Un inventaire détaillé des équipements et du mobilier doit être tenu, afin d'en suivre les mouvements. Aucun meuble ou matériel ne doit être introduit dans ce type de 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 des lignes de communication dans les zones protégées sur le plan technique n'est pas permise sans autorisation préalable de l'autorité compétente.

19. RÈGLES GÉNÉRALES RELATIVES AU BESOIN D'EN CONNAÎTRE ET AUX HABILITATIONS DE SÉCURITÉ DU PERSONNEL DE L'UE

19.1. **Généralités**

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 ►M1 TRES SECRET UE/EU TOP SECRET ◄ et CONFIDENTIEL UE n'est autorisé qu'aux personnes en possession de l'habilitation de sécurité correspondante.

La détermination du besoin d'en connaître incombe au service dans lequel la personne concernée est appelée à travailler.

Chaque service est responsable des demandes d'habilitation pour son personnel.

La procédure se concrétise par la délivrance d'un «certificat personnel d'habilitation de sécurité» précisant le degré de classification des informations auxquelles la personne habilitée peut avoir accès et la date de péremption de l'habilitation.

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

Les personnes autres que les fonctionnaires ou autres agents, tels que les contractants externes, experts ou consultants, 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.

L'accès public demeure régi par le règlement (CE) nº 1049/2001.

19.2. **Règles spécifiques concernant l'accès aux informations classifiées ►M1 TRES SECRET UE/EU TOP SECRET ◄**

Toute personne ayant à connaître des informations classifiées ►M1 TRES SECRET UE/EU TOP SECRET ◄ doit avoir fait l'objet, au préalable, d'une procédure d'habilitation permettant l'accès à ces informations.

Toute personne qui doit avoir accès aux informations ►M1 TRES SECRET UE/EU TOP SECRET ◄ doit être nommément désignée par le membre de la Commission chargé des questions de sécurité et son nom doit être conservé dans le bureau d'ordre ►M1 TRES SECRET UE/EU TOP SECRET ◄ approprié. Ce bureau d'ordre est créé et tenu par la ►M2 direction de la sécurité de la Commission ◄.

▼B

Toute personne autorisée à accéder à des informations ►M1 TRES SECRET UE/EU TOP SECRET ◄ doit signer au préalable une attestation reconnaissant qu'elle a été instruite des procédures de sécurité de la Commission et qu'elle comprend parfaitement sa responsabilité particulière en ce qui concerne la protection des informations ►M1 TRES SECRET UE/EU TOP SECRET ◄ ainsi que les conséquences prévues par la réglementation de l'Union européenne et les dispositions législatives ou administratives nationales lorsque des informations classifiées parviennent en des mains non autorisées, que ce soit à la suite d'une action délibérée ou d'une négligence.

En ce qui concerne les personnes ayant accès à des informations ►M1 TRES 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 informer le service organisateur de la réunion qu'elles sont autorisées à accéder aux informations ►M1 TRES SECRET UE/EU TOP SECRET ◄.

Les noms de toutes les personnes qui ne sont plus employées à des fonctions nécessitant l'accès aux informations ►M1 TRES SECRET UE/EU TOP SECRET ◄ sont être rayés de la liste correspondante. De plus, l'attention de toutes ces personnes doit être attirée à nouveau sur leurs responsabilités particulières quant à la protection des informations ►M1 TRES SECRET UE/EU TOP SECRET ◄. Elles doivent également signer une déclaration par laquelle elles s'engagent à ne pas utiliser ni divulguer les informations ►M1 TRES SECRET UE/EU TOP SECRET ◄ dont elles ont eu connaissance.

19.3. **Règles spécifiques concernant l'accès aux informations classifiées ►M1 TRES SECRET UE/EU TOP SECRET ◄ et CONFIDENTIEL UE**

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.

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

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 organisateur de la réunion qu'elle est autorisée à accéder à de telles informations.

19.4. **Règles spécifiques concernant l'accès aux informations classifiées RESTREINT UE**

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

19.5. **Mutations**

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 de façon réglementaire.

Lorsqu'un membre du personnel est affecté à un poste impliquant la manipulation de matériel classifié UE, il reçoit du responsable local de la sécurité les instructions appropriées.

19.6. **Instructions spéciales**

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 qui s'imposent dans leurs relations avec la presse et les représentants des groupes défendant des intérêts particuliers;

▼B

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.

Toutes les personnes ordinairement 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.

La Commission ne prévoit pas de consignes de sécurité 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. Il incombe toutefois à la ►M2 direction de la sécurité de la Commission ◄ d'informer les fonctionnaires et autres agents se trouvant sous sa responsabilité des règles qu'ils peuvent avoir à observer en matière de voyages.

20. PROCÉDURE D'HABILITATION DE SÉCURITÉ POUR LES FONCTIONNAIRES ET AUTRES AGENTS DE LA COMMISSION

a) Seuls les fonctionnaires et autres agents de la Commission ou les personnes travaillant au sein de la Commission qui, en raison de leurs fonctions et pour des nécessités de service, ont besoin de prendre connaissance d'informations classifiées détenues par la Commission ou d'en faire usage, ont accès auxdites informations.

b) Pour pouvoir accéder aux informations classifiées «►M1 TRES 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 décrite aux points c) et d) de la présente section.

c) 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 i) à n).

d) Le ►M2 directeur de la direction de la sécurité de la Commission ◄ est responsable de l'octroi des autorisations visées aux points a), b) et c).

e) Il accorde 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 i) à n).

f) La ►M2 direction de la sécurité de la Commission ◄ tient une liste actualisée de tous les postes sensibles, fournie par les services concernés de la Commission, et de toutes les personnes ayant reçu une autorisation (temporaire).

g) 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 conformément à la procédure visée au point e).

h) L'autorisation est retirée par le ►M2 directeur de la direction de la sécurité de la Commission ◄ dès lors que ce dernier le juge opportun. Toute décision de retrait est notifiée à la personne concernée, qui peut demander à être entendue par le ►M2 directeur de la direction de la sécurité de la Commission ◄, ainsi qu'à l'autorité nationale compétente.

▼B

i) L'enquête de sécurité est effectuée avec le concours de la personne concernée et à la demande du ►M2 directeur de la direction de la sécurité de la Commission ◄. L'administration nationale compétente aux fins de l'enquête de sécurité est celle de l'État membre dont l'intéressé(e) est ressortissant(e). Lorsque la personne concernée n'est pas ressortissant d'un État membre de l'UE, le ►M2 directeur de la direction de la sécurité de la Commission ◄ demande une enquête de sécurité à l'État membre de l'UE dans lequel la personne est domiciliée ou réside habituellement.

j) Dans le cadre de l'enquête, la personne concernée est tenue de remplir une notice individuelle d'information.

k) Le ►M2 directeur de la direction de la sécurité de la Commission ◄ spécifie dans sa demande le type et le niveau de classification des informations dont 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.

l) 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 voies de recours.

m) Lorsque les autorités nationales compétentes des États membres émettent un avis positif, le ►M2 directeur de la direction de la sécurité de la Commission ◄ peut octroyer l'autorisation à la personne concernée.

n) Lorsque les autorités nationales compétentes émettent un avis négatif, la personne concernée en est informée et peut demander à être entendue par le ►M2 directeur de la direction de la sécurité de la Commission ◄. S'il le juge nécessaire, ce dernier peut demander aux autorités nationales compétentes tout éclaircissement complémentaire qu'elles sont en mesure de fournir. En cas de confirmation de l'avis négatif, l'autorisation ne peut être accordée.

o) Toute personne autorisée au sens des points d) et e) 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.

p) Le ►M2 directeur de la direction de la sécurité de la Commission ◄ prend toute mesure nécessaire pour appliquer les dispositions de la présente section, notamment celles qui concernent l'accès à la liste des personnes autorisées.

q) À titre exceptionnel et en raison des nécessités du service, le ►M2 directeur de la direction de la sécurité de la Commission ◄ 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 i).

r) Les autorisations provisoires et temporaires ainsi octroyées ne donnent pas accès aux informations ►M1 TRES SECRET UE/EU TOP SECRET ◄, réservé aux fonctionnaires qui ont effectivement fait l'objet d'une enquête de sécurité dont l'issue a été positive, conformément au point i). En attendant les résultats de l'enquête de sécurité, les fonctionnaires qui doivent être habilités au niveau ►M1 TRES SECRET UE/EU TOP SECRET ◄, peuvent être autorisés, à titre temporaire et provisoire, à accéder aux informations classifiées jusqu'au niveau SECRET UE inclus.

▼B

21. PRÉPARATION, RÉPARTITION, TRANSMISSION, MESURES DE SÉCURITÉ RELATIVES AUX COURRIERS, EXEMPLAIRES SUPPLÉMENTAIRES, TRADUCTIONS ET EXTRAITS DE DOCUMENTS CLASSIFIÉS DE L'UE

21.1. **Préparation**

1. Les classifications sont appliquées comme prescrit à la section 16. Pour les documents de niveau CONFIDENTIEL UE et au-delà, la classification apparaît, centrée, en tête et en pied de chaque page. Les pages sont toutes numérotées. Chaque document classifié de l'UE doit porter un numéro de référence ainsi qu'une date. Pour les documents ►**M1** TRES SECRET UE/EU TOP SECRET ◄ et SECRET UE, ce numéro de référence est 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-delà doit donner la liste complète des annexes et pièces jointes.

2. Les documents classifiés CONFIDENTIEL UE et au-delà 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.

3. Les dispositions relatives à la production de documents classifiés à l'aide de moyens informatiques sont énoncées à la section 25.

21.2. **Diffusion**

1. 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. Il appartient à l'autorité d'origine d'indiquer la liste de diffusion initiale.

2. La diffusion des documents ►**M1** TRES SECRET UE/EU TOP SECRET ◄ s'effectue par la voie des bureaux d'ordre ►**M1** TRES SECRET UE/EU TOP SECRET ◄ (voir section 22.2). Dans le cas de messages ►**M1** TRES 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.

3. Les documents classifiés SECRET UE et en deçà 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.

4. Tout document classifié CONFIDENTIEL UE et au-delà fait l'objet d'un enregistrement à l'entrée et à la sortie d'une DG ou d'un service. Cette tâche incombe au bureau d'ordre local chargé des informations classifiées de l'UE dans le service concerné. 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 (voir section 22.1).

21.3. **Transmission/transport de documents classifiés de l'UE**

21.3.1. *Emballages et récépissés*

1. Les documents classifiés CONFIDENTIEL UE et au-delà 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.

▼B

2. Seul l'agent contrôleur du bureau d'ordre (voir section 22.1), 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 (voir section 22.1), 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.

3. 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.

4. 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.

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

21.3.2. *Transmission au sein d'un bâtiment ou d'un groupe de bâtiments*

À l'intérieur d'un même bâtiment ou groupe de bâtiments, les documents classifiés peuvent être transmis dans une enveloppe scellée 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.

21.3.3. *Transmission à l'intérieur d'un même pays*

1. La transmission des documents ►**M1** TRES 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 accéder aux informations ►**M1** TRES SECRET UE/EU TOP SECRET ◄.

2. Chaque fois qu'il est fait appel à un service de messagerie pour le transport d'un document ►**M1** TRES 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 dans le présent chapitre. Les services de messagerie doivent disposer d'un personnel suffisant pour que les paquets contenant des documents ►**M1** TRES SECRET UE/EU TOP SECRET ◄ demeurent sous le contrôle direct et permanent d'un responsable.

3. Exceptionnellement, des documents ►**M1** TRES 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 accéder à ces documents ►**M1** TRES SECRET UE/EU TOP SECRET ◄;

   b) le mode de transport soit conforme aux règles applicables à la transmission de documents de niveau ►**M1** TRES SECRET UE/EU TOP SECRET ◄;

   c) le porteur ne se sépare en aucun cas des documents ►**M1** TRES 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 ►**M1** TRES SECRET UE/EU TOP SECRET ◄ détenteur et notée dans un registre, afin de permettre une vérification lors du retour de ces documents.

4. 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 du pays en matière de sécurité, 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.

▼B

5. La ►M2 direction de la sécurité de la Commission ◄ doit élaborer, sur la base de cette réglementation, des instructions relatives au transport individuel de documents classifiés de l'UE. Le porteur est invité à lire et parapher ces instructions. Celles-ci précisent 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 18;

   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 et ne peuvent pas non plus être déposés dans les coffres d'hôtels ou laissés 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.

21.3.4. *Transmission d'un État à un autre*

1. Les matériels classifiés CONFIDENTIEL UE ou à un niveau supérieur sont transmis d'un État membre à un autre par les services du courrier diplomatique ou militaire.

2. 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.

3. Le membre de la Commission chargé des questions de sécurité peut autoriser le transport par une personne lorsqu'on ne peut utiliser ni le courrier diplomatique ni le courrier militaire, ou lorsque leur utilisation entraînerait un retard risquant de compromettre des opérations de l'UE et que le matériel est requis d'urgence par son destinataire. La ►M2 direction de la sécurité de la Commission ◄ rédige des instructions applicables au 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 dispose de l'habilitation de sécurité appropriée;

   b) tous les matériels ainsi transportés soient enregistrés dans le service 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 trouverait;

   d) le porteur soit muni d'un certificat de courrier et/ou d'un ordre de mission reconnu par tous les États membres 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 18;

   h) les documents 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 et ne soient pas non plus déposés dans les coffres d'hôtels ou laissés 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.).

▼B

4. 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.

21.3.5. *Transmission/transport de documents classifiés «RESTREINT UE»*

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

21.4. **Mesures de sécurité relatives aux courriers**

Tous les courriers et messagers utilisés pour le transport des documents SECRET UE et CONFIDENTIEL UE doivent avoir reçu une habilitation de sécurité appropriée.

21.5. **Transmission par voie électronique ou d'autres moyens techniques**

1. 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 25.

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

21.6. **Exemplaires supplémentaires et traductions et extraits de documents classifiés de l'UE**

1. Seule l'autorité d'origine peut autoriser la duplication ou la traduction de documents ►**M1** TRES SECRET UE/EU TOP SECRET ◄.

2. Si des personnes ne possédant pas l'habilitation ►**M1** TRES SECRET UE/EU TOP SECRET ◄ ont besoin d'informations contenues dans un document ►**M1** TRES SECRET UE/EU TOP SECRET ◄ mais n'ont pas elles-mêmes ce niveau de classification, le chef du bureau d'ordre ►**M1** TRES SECRET UE/EU TOP SECRET ◄ (voir section 22.2) peut être autorisé à réaliser le nombre d'extraits nécessaires de ce document. Il prend simultanément les mesures requises pour que ces documents reçoivent une classification de sécurité appropriée.

3. Les reproductions et traductions de documents SECRET UE et d'un niveau de classification plus bas peuvent être faites par le destinataire, dans le cadre des présentes dispositions de sécurité et à condition d'observer 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.

22. BUREAUX D'ORDRE, REGROUPEMENTS, CONTRÔLES, ARCHIVAGE ET DESTRUCTION DE DOCUMENTS CLASSIFIÉS DE L'UE

22.1. **Bureaux d'ordre locaux chargés des documents classifiés de l'UE**

1. Au sein de chaque service de la Commission, en fonction des nécessités, un ou plusieurs bureaux d'ordre est mis en place pour la gestion des informations classifiées de l'UE. Ils ont pour tâche d'enregistrer, de reproduire, de diffuser, d'archiver et de détruire les documents classifiés SECRET UE et CONFIDENTIEL UE.

2. Si un service ne dispose pas de bureau d'ordre local pour les informations classifiées de l'UE, c'est le bureau d'ordre local du Secrétariat général qui en assume la fonction.

3. Les bureaux d'ordre locaux pour les informations classifiées de l'UE dépendent du chef d'unité dont ils reçoivent leurs instructions. Ils sont dirigés par un agent contrôleur (RCO).

▼B

4. Ils sont placés sous la supervision du responsable local de la sécurité pour ce qui concerne l'application des dispositions relatives à la manipulation de documents classifiés de l'UE et la mise en œuvre des mesures de sécurité correspondantes.

5. Les fonctionnaires en poste dans les bureaux d'ordre locaux pour les informations classifiées de l'UE ont accès à ces informations dans les conditions définies à la section 20.

6. Sous l'autorité des chefs d'unité concernés, les bureaux d'ordre locaux pour les ICUE:

   a) gèrent les opérations relatives à l'enregistrement, la reproduction, la traduction, la transmission, l'expédition et la destruction des informations classifiées de l'UE;

   b) tiennent à jour le registre concernant les informations classifiées;

   c) interrogent périodiquement les émetteurs sur la nécessité de maintenir la classification de ces informations.

7. Les bureaux locaux pour les ICUE tiennent un registre des données suivantes:

   a) la date d'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) l'objet;

   g) le numéro;

   h) le nombre d'exemplaires diffusés;

   i) les renseignements relatifs à l'élaboration d'inventaires des informations classifiées soumises au service;

   j) le registre des opérations de déclassification et de déclassement des informations classifiées.

8. Les règles générales exposées à la section 21 s'appliquent aux bureaux d'ordre locaux de la Commission, sans préjudice des éventuelles modifications apportées par les dispositions spécifiques de la présente section.

22.2. **Le bureau d'ordre ►M1 TRES SECRET UE/EU TOP SECRET ◄**

22.2.1. *Généralités*

1. Un bureau d'ordre ►M1 TRES SECRET UE/EU TOP SECRET ◄ assure l'enregistrement, le traitement et la diffusion des documents ►M1 TRES SECRET UE/EU TOP SECRET ◄ conformément aux présentes règles de sécurité. Le bureau d'ordre ►M1 TRES SECRET UE/EU TOP SECRET ◄ est dirigé par l'agent contrôleur ►M1 TRES SECRET UE/EU TOP SECRET ◄.

2. Le bureau d'ordre central ►M1 TRES SECRET UE/EU TOP SECRET ◄ représente la principale autorité de réception et de diffusion à l'intérieur de la Commission et pour les échanges avec les autres institutions de l'UE, les États membres, les organisations internationales et les États tiers avec lesquels la Commission 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 ►M1 TRES SECRET UE/EU TOP SECRET ◄; ils tiennent à jour la situation de chacun des documents en circulation dont ils ont la charge.

▼B

4. Les bureaux d'ordre ►M1 TRES SECRET UE/EU TOP SECRET ◄ subordonnés sont créés comme indiqué à la section 22.2.3 pour répondre à un besoin permanent et sont rattachés à un bureau d'ordre central ►M1 TRES SECRET UE/EU TOP SECRET ◄. S'il n'existe qu'un besoin de consultation temporaire et occasionnel de documents ►M1 TRES SECRET UE/EU TOP SECRET ◄, ces documents peuvent être communiqués sans création d'un bureau d'ordre ►M1 TRES SECRET UE/EU TOP SECRET ◄ subordonné, sous réserve que les règles établies garantissent qu'ils resteront sous le contrôle du bureau d'ordre ►M1 TRES SECRET UE/EU TOP SECRET ◄ approprié, et sous réserve du respect de toutes les mesures de sécurité physiques et de toutes celles concernant le personnel.

5. Les bureaux d'ordre subordonnés ne peuvent transmettre des documents ►M1 TRES SECRET UE/EU TOP SECRET ◄ directement à d'autres bureaux d'ordre subordonnés au même bureau d'ordre ►M1 TRES SECRET UE/EU TOP SECRET ◄ central sans l'autorisation expresse de ce dernier.

6. Tous les échanges de documents ►M1 TRES 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 centraux ►M1 TRES SECRET UE/EU TOP SECRET ◄.

22.2.2. *Le bureau d'ordre central ►M1 TRES SECRET UE/EU TOP SECRET ◄*

En tant qu'agent contrôleur, le chef du bureau d'ordre central ►M1 TRES SECRET UE/EU TOP SECRET ◄ a pour responsabilités:

a) d'assurer la transmission des documents ►M1 TRES SECRET UE/EU TOP SECRET ◄ conformément aux règles définies à la section 21.3;

b) de tenir à jour la liste de tous ses bureaux d'ordre ►M1 TRES SECRET UE/EU TOP SECRET ◄ subordonnés avec les noms et les signatures des agents contrôleurs désignés et de leurs adjoints autorisés;

c) de conserver les récépissés des bureaux d'ordre pour tous les documents ►M1 TRES SECRET UE/EU TOP SECRET ◄ diffusés par le bureau d'ordre central;

d) de tenir un état des documents ►M1 TRES SECRET UE/EU TOP SECRET ◄ détenus et diffusés;

e) de tenir à jour une liste de tous les bureaux d'ordre centraux ►M1 TRES SECRET UE/EU TOP SECRET ◄ avec lesquels il correspond normalement, comportant les noms et signatures des agents contrôleurs désignés et de leurs adjoints autorisés;

f) d'assurer la sécurité matérielle de tous les documents ►M1 TRES SECRET UE/EU TOP SECRET ◄ détenus dans le bureau d'ordre, conformément aux prescriptions énoncées à la section 18.

22.2.3. *Bureaux d'ordre ►M1 TRES SECRET UE/EU TOP SECRET ◄ subordonnés*

En tant qu'agent contrôleur, le chef d'un bureau d'ordre ►M1 TRES SECRET UE/EU TOP SECRET ◄ subordonné a pour responsabilités:

a) d'assurer la transmission des documents ►M1 TRES SECRET UE/EU TOP SECRET ◄ conformément aux règles définies à la section 21.3;

b) de tenir à jour la liste de toutes les personnes autorisées à accéder aux informations ►M1 TRES SECRET UE/EU TOP SECRET ◄ sous son contrôle;

c) de diffuser les documents ►M1 TRES 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 ►M1 TRES SECRET UE/EU TOP SECRET ◄ détenus ou en circulation sous son contrôle, ou qui ont été transmis à d'autres bureaux d'ordre ►M1 TRES SECRET UE/EU TOP SECRET ◄, et de conserver tous les récépissés correspondants;

▼B

e) de tenir à jour la liste des bureaux d'ordre ►M1 TRES SECRET UE/EU TOP SECRET ◄ avec lesquels il est autorisé à échanger des documents ►M1 TRES 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 ►M1 TRES SECRET UE/EU TOP SECRET ◄ détenus dans le bureau d'ordre subordonné, conformément aux prescriptions énoncées à la section 18.

22.3. **Inventaires, regroupements et contrôles de documents classifiés de l'UE**

1. Tous les ans, chaque bureau d'ordre ►M1 TRES SECRET UE/EU TOP SECRET ◄ tel que visé à la présente section procède à un inventaire détaillé des documents ►M1 TRES SECRET UE/EU TOP SECRET ◄. 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 ►M1 TRES 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. Pour le 1er avril de chaque année au plus tard, les bureaux d'ordre subordonnés adressent les résultats de leur inventaire annuel au membre de la Commission chargé des questions de sécurité.

2. Les bureaux d'ordre ►M1 TRES SECRET UE/EU TOP SECRET ◄ subordonnés adressent au bureau d'ordre central dont ils relèvent, à la date fixée par ce dernier, les résultats de leur inventaire annuel.

3. Les documents classifiés de l'UE d'un niveau inférieur à ►M1 TRES SECRET UE/EU TOP SECRET ◄ doivent faire l'objet de vérifications internes conformément aux directives données par le membre de la Commission chargé des questions de sécurité.

4. 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.

22.4. **Archivage d'informations classifiées de l'UE**

1. Les informations classifiées de l'UE doivent être archivées conformément à toutes les dispositions pertinentes de la section 18.

2. Afin de limiter les problèmes d'archivage, les agents contrôleurs de tous les bureaux d'ordre sont autorisés à faire microfilmer les documents ►M1 TRES 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 en cours de validité correspondant à la classification appropriée;

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

   c) la mise sur microfilm/l'archivage de tout document ►M1 TRES 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 ►M1 TRES SECRET UE/EU TOP SECRET ◄, SECRET UE ou CONFIDENTIEL UE;

▼B

e) la mise sur microfilm/l'archivage d'un document ►M1 TRES SECRET UE/EU TOP SECRET ◄ ou SECRET UE soit clairement indiqué(e) dans 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 à la section 22.5.

3. Ces règles s'appliquent également à tout autre moyen d'archivage autorisé, tels que les supports électromagnétiques et les disques optiques.

22.5. **Destruction des documents classifiés de l'UE**

1. 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 ►M1 TRES 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 ►M1 TRES SECRET UE/EU TOP SECRET ◄ et par un témoin qui doit être habilité ►M1 TRES 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 ►M1 TRES SECRET UE/EU TOP SECRET ◄, y compris tous les rebuts classifiés résultant de l'élaboration de ces documents (exemplaires endommagés, brouillons, notes dactylographiées, disquettes, etc.), doivent être détruits sous la surveillance d'un responsable du registre ►M1 TRES SECRET UE/EU TOP SECRET ◄, par incinération, réduction en pulpe, lacération en bandes ou division en fragments non identifiables rendant impossible toute reconstitution.

2. 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 1 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.

3. 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 1 c). Leur destruction est enregistrée conformément aux instructions du membre de la Commission chargé des questions de sécurité.

4. Les documents RESTREINT UE sont détruits par le bureau d'ordre qui en a la charge ou par l'utilisateur, conformément aux instructions du membre de la Commission chargé des questions de sécurité.

22.6. **Destruction en cas d'urgence**

1. Les services de la Commission 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 émettent les consignes qu'ils jugent appropriées pour éviter que des informations classifiées de l'UE ne tombent entre les mains de personnes non autorisées.

▼B

2. 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 ►M1 TRES SECRET UE/EU TOP SECRET ◄, et notamment des matériels de chiffrement, dont la prise en charge doit avoir la priorité sur toutes les autres tâches.

3. Les mesures à prendre pour la sauvegarde et la destruction d'urgence des matériels de chiffrement font l'objet d'instructions spécifiques

4. Les instructions doivent être disponibles immédiatement dans une enveloppe scellée. Les moyens/outils de destruction des matériels concernés doivent être disponibles.

23. MESURES DE SÉCURITÉ À APPLIQUER À L'OCCASION DES RÉUNIONS SPÉCIFIQUES TENUES EN DEHORS DES LOCAUX DE LA COMMISSION ET METTANT EN JEU DES INFORMATIONS CLASSIFIÉES DE L'UE

23.1. **Généralités**

Lorsque les réunions de la Commission ou d'autres réunions importantes ont lieu en dehors des locaux de la Commission, et que les exigences de sécurité particulières découlant du niveau de sensibilité élevé des dossiers ou informations traités le justifient, il convient de prendre les mesures de sécurité décrites ci-après. 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.

23.2. **Responsabilités**

23.2.1. *La* ►M2 *direction de la sécurité de la Commission* ◄

La ►M2 direction de la sécurité de la Commission ◄ coopère avec les autorités compétentes de l'État membre sur le territoire duquel se déroule la réunion (État membre d'accueil) afin d'assurer la sécurité des réunions de la Commission ou autres réunions importantes concernées, ainsi que la sécurité physique des délégués et de leurs collaborateurs. En matière de protection de la sécurité, la ►M2 direction de la sécurité de la Commission ◄ veille en particulier 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 de la Commission pour la réception et l'envoi de messages classifiés de l'UE. Il est également demandé à l'État membre d'accueil d'assurer, le cas échéant, l'accès à des systèmes téléphoniques protégés.

La ►M2 direction de la sécurité de la Commission ◄ joue un rôle de conseiller en matière de sécurité pour la préparation de la réunion; elle doit y être représentée pour aider et conseiller, le cas échéant, le responsable de la sécurité de la réunion et les délégations.

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 de la ►M2 direction de la sécurité de la Commission ◄, le cas échéant.

23.2.2. *Le responsable de la sécurité de la réunion*

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 portent d'une manière générale sur:

a) 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;

▼B

b) 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;

c) la coordination permanente avec les autorités compétentes de l'État membre d'accueil et avec la ►M2 direction de la sécurité de la Commission ◄;

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

23.3. **Mesures de sécurité**

23.3.1. *Zones de sécurité*

Il y a lieu d'établir 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 de la Commission, 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.

23.3.2. *Laissez-passer*

Le responsable de la sécurité de la réunion établit 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.

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.

Outre les participants munis de badges, il y a lieu d'admettre le moins de personnes possible sur le lieu de la réunion. Au cours de la réunion, le responsable de la sécurité de la réunion ne permet aux délégations nationales de recevoir des visiteurs que sur demande expresse. 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.

23.3.3. *Contrôle des appareils photographiques et des appareils d'enregistrement*

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.

23.3.4. *Contrôle des porte-documents, ordinateurs portatifs et paquets*

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.

▼B

23.3.5. *Sécurité technique*

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.

23.3.6. *Documents des délégations*

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.

23.3.7. *Conservation des documents en lieu sûr*

Lorsque 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.

23.3.8. *Vérification des bureaux*

Le responsable de la sécurité de la réunion doit veiller à ce que les bureaux de la Commission 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 prend les mesures appropriées.

23.3.9. *Élimination des rebuts classifiés de l'UE*

Tous les rebuts doivent être considérés comme documents classifiés de l'UE et la Commission 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, la Commission 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.

À la fin de la réunion, tous les documents détenus par la Commission ou les délégations et devenus inutiles sont traités comme rebuts. Une fouille approfondie des bureaux de la Commission 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 22.5.

24. INFRACTIONS À LA SÉCURITÉ ET COMPROMISSION DES INFORMATIONS CLASSIFIÉES DE L'UE

24.1. **Définitions**

Une infraction à la sécurité est un acte ou une omission contraire à une règle de sécurité de la Commission et susceptible de mettre en danger ou de compromettre des informations classifiées de l'UE.

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.

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.

24.2. **Dénonciation des infractions à la sécurité**

Toutes les personnes amenées à manipuler des informations classifiées de l'UE doivent recevoir une information complète sur leurs responsabilités dans ce domaine. Elles signalent immédiatement toute infraction à la sécurité qu'elles ont pu remarquer.

▼B

Lorsqu'un responsable local de la sécurité ou un responsable de la sécurité d'une réunion 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, il doit agir rapidement pour:

a) protéger les éléments de preuve;

b) établir les faits;

c) évaluer et réduire au minimum les dommages;

d) éviter que les faits ne se reproduisent;

e) informer les autorités compétentes des conséquences de l'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.

Dès qu'une infraction à la sécurité a été notifiée, chaque autorité de sécurité a le devoir d'en avertir immédiatement la ►M2 direction de la sécurité de la Commission ◄.

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

Dès qu'il est informé d'une infraction à la sécurité, le membre de la Commission chargé des questions de sécurité:

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.

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

24.3. **Actions en justice**

Toute personne dont la responsabilité est engagée dans la compromission d'informations classifiées de l'UE est passible de sanctions disciplinaires conformément à la réglementation applicable, surtout le titre VI du statut, et sans préjudice d'autres poursuites en justice.

Le cas échéant, sur la base du rapport visé à la section 24.2, le membre de la Commission chargé des questions de sécurité prend toutes les mesures qui s'imposent pour permettre aux autorités nationales compétentes d'engager des procédures pénales.

▼B

25. PROTECTION DES INFORMATIONS CLASSIFIÉES DE L'UE TRANSITANT PAR DES SYSTÈMES DE COMMUNICATION ET D'INFORMATION

25.1. **Introduction**

25.1.1. *Généralités*

La politique de sécurité et les exigences en la matière s'appliquent à tous les systèmes et réseaux de communication et d'information (ci-après dénommés «systèmes») qui traitent des informations CONFIDENTIEL UE ou de classification supérieure. Ils sont appliqués en complément des dispositions de la décision C(95) 1510 final de la Commission du 23 novembre 1995 relative à la protection des systèmes d'information.

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.

La politique de sécurité appliquée par la Commission en matière de technologies de l'information comporte les éléments suivants:

— appartenance, en tant que partie intégrante, à la politique globale de sécurité et complète tous les éléments relatifs à la sécurité de l'information, de la sécurité du personnel et de la sécurité physique,

— répartition des responsabilités entre l'autorité d'exploitation des systèmes techniques, ceux des informations classifiées de l'UE stockées ou traitées dans des systèmes techniques, les spécialistes de la sécurité informatique et les utilisateurs,

— description des principes de sécurité et des besoins de chaque système TI,

— approbation de ces principes et exigences par une autorité désignée,

— prise en compte des menaces et des vulnérabilités spécifiques au domaine des technologies de l'information.

25.1.2. *Vulnérabilité des systèmes et menaces éventuelles*

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.

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 nombreuses menaces. 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.

25.1.3. *But principal des mesures de sécurité*

Les mesures de sécurité énoncées dans la présente section ont pour principal objectif d'assurer la protection contre la divulgation non autorisée d'informations classifiées de l'UE (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 y a lieu que la ►M2 direction de la sécurité de la Commission ◄ spécifie les normes appropriées de protection classique, de même que les procédures et techniques adéquates de sécurité conçues spécialement pour chaque système.

▼B

25.1.4. *Énoncé des impératifs de sécurité propres à un système (SSRS)*

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, voir la section 25.3.4) et le propriétaire de l'information (voir la section 25.3.5), le cas échéant avec la contribution et l'assistance des responsables de projet et de la ►M2 direction de la sécurité de la Commission ◄ (agissant en tant qu'autorité INFOSEC-IA, voir la section 25.3.3), et approuvé par l'autorité d'homologation de sécurité (SAA, voir la section 25.3.2).

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 l'autorité d'homologation de sécurité (SAA).

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.

25.1.5. *Modes d'exploitation de sécurité*

Tous les systèmes qui traitent des informations CONFIDENTIEL UE ou de 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;

c) mode multiniveau.

25.2. **Définitions**

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;

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

▼B

Par «responsable de la sécurité informatique au niveau central» (CISO), on entend le fonctionnaire qui, au sein d'un service informatique central, coordonne et supervise les mesures de sécurité pour les systèmes organisés sur un mode centralisé.

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.

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.

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 le blocage de l'accès.

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.

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.

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.

Par «propriétaire de l'information» (IO), on entend l'autorité (chef d'unité) qui a la responsabilité de la création, du traitement et de l'utilisation de l'information, ce qui comprend la désignation des personnes autorisées à y accéder.

▼B

Par «sécurité de l'information» (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.

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.

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.

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).

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 (TSO).

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

▼B

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.

On entend par «responsable de la sécurité informatique au niveau local» (LISO) le fonctionnaire qui, dans un service de la Commission, est chargé de coordonner et de superviser les mesures de sécurité dans les limites de son domaine.

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.

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.

Par «procédures d'exploitation de sécurité», on entend les procédures élaborées par le propriétaire des systèmes techniques et définissant les principes à observer en matière de sécurité, les procédures d'exploitation à appliquer et les responsabilités du personnel.

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.

▼B

On entend par «énoncé des impératifs de sécurité propres à un système» (SSRS) 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 de la Commission 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.

On entend par «propriétaire des systèmes techniques» (TSO) l'autorité responsable de la mise en place, de la maintenance, de l'exploitation et de la fermeture d'un système.

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 et la conductivité.

25.3. **Responsabilités en matière de sécurité**

25.3.1. *Généralités*

Les responsabilités consultatives du groupe consultatif sur la politique de sécurité de la Commission, définies dans la section 12, incluent les questions INFOSEC. Ce groupe organise ses activités de manière à pouvoir fournir des conseils de spécialistes concernant les questions précitées.

La ►M2 direction de la sécurité de la Commission ◄ est chargée de publier des règles INFOSEC détaillées sur la base des dispositions du présent chapitre.

En cas de problème de sécurité (incidents, infractions, etc.), la ►M2 direction de la sécurité de la Commission ◄ prend immédiatement des mesures.

La ►M2 direction de la sécurité de la Commission ◄ dispose d'une unité INFOSEC.

25.3.2. *L'autorité d'homologation de sécurité (SAA)*

Le ►M2 directeur de la direction de la sécurité de la Commission ◄ est l'autorité d'homologation de sécurité (SAA) de la Commission. La SAA est responsable de l'organisation générale de la sécurité et des domaines INFOSEC spécialisés, à savoir la sécurité des communications, la sécurité Crypto et la sécurité TEMPEST.

Elle est chargée de veiller à la conformité des systèmes avec la politique de sécurité de la Commission. L'une de ses tâches consiste à prononcer l'homologation d'un système en vue du traitement des informations classifiées de l'UE à un niveau de classification déterminé dans son environnement d'exploitation.

Tous les systèmes exploités dans les locaux de la Commission relèvent de la compétence de la SAA de la Commission. Lorsque différents éléments d'un même système sont du ressort de la SAA de la Commission et d'autres SAA, toutes les parties concernées peuvent désigner un comité mixte d'homologation, la coordination étant assurée par la SAA de la Commission.

25.3.3. *L'autorité INFOSEC (IA)*

Le chef de l'unité INFOSEC de la ►M2 direction de la sécurité de la Commission ◄ est l'autorité INFOSEC de la Commission. L'autorité INFOSEC est chargée:

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

— de contribuer à l'élaboration du SSRS,

▼B

— d'examiner le SSRS pour assurer sa cohérence avec les présentes règles de sécurité ainsi qu'avec 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 en matière d'homologation,

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

— de fournir des conseils techniques dans le cadre des enquêtes sur les incidents INFOSEC,

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

25.3.4. *Le propriétaire des systèmes techniques (TSO)*

La responsabilité de la mise en œuvre des contrôles et du fonctionnement des dispositifs de sécurité spéciaux d'un système est assurée par le propriétaire de ce système, le propriétaire des systèmes techniques (TSO). En ce qui concerne les systèmes gérés au niveau central, un responsable principal de la sécurité informatique (CISO) est nommé. Chaque service nomme, le cas échéant, un responsable local de la sécurité informatique (LISO). La responsabilité d'un TSO inclut l'établissement des procédures d'exploitation de sécurité (SecOP). Il l'exerce pendant toute la durée de vie du système, de la conception du projet à son arrêt définitif.

Le TSO spécifie les normes et pratiques de sécurité auxquelles le fournisseur du système doit se conformer.

Le cas échéant, il peut déléguer une partie de ses responsabilités à un responsable local de la sécurité informatique. Une seule et même personne peut remplir les différentes fonctions INFOSEC.

25.3.5. *Le propriétaire de l'information (IO)*

Le propriétaire de l'information (IO) est responsable des informations classifiées de l'Union européenne (et autres informations) qui doivent être introduites, traitées et produites dans les systèmes techniques. Il définit les exigences en matière d'accès à ces informations dans les systèmes. Il peut déléguer cette responsabilité à un gestionnaire de l'information ou à un gestion de base de données de son secteur.

25.3.6. *Utilisateurs*

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.

25.3.7. *Formation INFOSEC*

Des actions d'apprentissage et de formation INFOSEC sont proposées à l'ensemble des membres du personnel qui en ont besoin.

25.4. **Mesures de sécurité non techniques**

25.4.1. *Sécurité du personnel*

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 de la Commission en vigueur.

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.

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.

▼B

Un fonctionnaire autorisé ou autre employé 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.

Les réglages de sécurité d'un système ne sont modifiés que par au moins deux personnes autorisées et pourvu qu'elles procèdent de concert.

25.4.2. *Sécurité physique*

Les zones TI et les zones de terminaux ou postes de travail distants (définies dans la section 25.2) 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.

25.4.3. *Contrôle des accès à un système*

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.

Lorsqu'ils ne sont plus utilisés à cette fin, les informations et les matériels de contrôle des accès doivent être détruits conformément aux dispositions de la section 25.5.4.

25.5. **Mesures de sécurité techniques**

25.5.1. *Sécurité des informations*

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.

Il incombe aux services de la Commission et aux personnes 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.

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.

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.

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.

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 approuvée par la SAA (voir points 25.5.4).

▼B

25.5.2. *Contrôle et comptabilisation des informations*

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 présentes règles de sécurité.

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.

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 et de relever les données ainsi disséminées. Pour les informations SECRET UE et au-delà, ces procédures comprennent des instructions particulières de comptabilisation des informations.

25.5.3. *Manipulation et contrôle des supports amovibles*

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.

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 aux présentes règles de sécurité.

25.5.4. *Déclassification et destruction des supports informatiques*

Les supports informatiques ayant servi à enregistrer des informations classifiées de l'UE peuvent être déclassés ou déclassifiés, à condition qu'une procédure approuvée par la SAA soit appliquée.

Les supports ayant contenu des informations ►M1 TRES SECRET UE/EU TOP SECRET ◄ ou d'une catégorie spéciale ne doivent pas être déclassifiés ni réutilisés.

Les supports qui ne peuvent être ni déclassifiés ni réutilisés sont détruits selon la procédure mentionnée ci-dessus.

25.5.5. *Sécurité des communications*

Le ►M2 directeur de la direction de la sécurité de la Commission ◄ est l'autorité Crypto.

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.

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

▼B

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 membre de la Commission chargé des questions de sécurité, après avis du groupe consultatif sur la politique de sécurité de la Commission. Pendant la transmission, la confidentialité des informations CONFIDENTIEL UE ou RESTREINT UE doit être protégée par des méthodes ou des produits cryptographiques agréés par l'autorité Crypto de la Commission, après avis du groupe consultatif sur la politique de sécurité de la Commission.

Les règles détaillées applicables à la transmission d'informations classifiées de l'UE doivent figurer dans des instructions de sécurité spécifiques approuvées par la ►**M2** direction de la sécurité de la Commission ◄, après avis du groupe consultatif sur la politique de sécurité de la Commission.

Dans des circonstances exceptionnelles, les informations classifiées 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 du propriétaire de l'information et soit dûment enregistrée par lui. 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.

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.

25.5.6. *Mesures de sécurité concernant l'installation et le rayonnement*

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.

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

Les contre-mesures TEMPEST sont examinées et approuvées par l'autorité TEMPEST (voir le point 25.3.2).

25.6. **Sécurité pendant le traitement**

25.6.1. *Procédures d'exploitation de sécurité (SecOP)*

Les procédures d'exploitation de sécurité (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 du propriétaire des systèmes techniques (TSO).

25.6.2. *Protection et gestion de la configuration des logiciels*

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.

▼B

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 le TSO.

25.6.3. *Détection de la présence de logiciels malveillants ou de virus informatiques*

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

Tout support informatique pénétrant dans la Commission 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.

25.6.4. *Maintenance*

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.

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.

25.7. **Acquisition**

25.7.1. *Généralités*

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 de l'un des États membres de l'UE, selon des critères internationalement reconnus (comme les Critères communs d'évaluation de la sécurité des technologies de l'information, cf. norme ISO 15408). Des procédures spécifiques sont exigées pour obtenir l'approbation de la CCAM.

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.

25.7.2. *Homologation*

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 la Commission et d'autres organisations, la Commission et les autorités de sécurité concernées doivent s'accorder sur la question de l'homologation.

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

25.7.3. *Évaluation et certification*

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.

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

▼B

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 du TSO.

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.

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.

25.7.4. *Contrôle systématique des dispositifs de sécurité pour la prorogation de l'homologation*

Le TSO établit des procédures de contrôle systématique garantissant que tous les dispositifs de sécurité du système sont toujours valables.

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 la SAA. Pour assurer le bon fonctionnement des dispositifs de sécurité, le TSO 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.

Tous les systèmes auxquels des dispositifs de sécurité ont été intégrés sont inspectés ou examinés périodiquement par la SAA. En ce qui concerne les systèmes qui traitent des informations ►**M1** TRES SECRET UE/EU TOP SECRET ◄, les inspections sont effectuées au moins une fois par an.

25.8. **Utilisation temporaire ou occasionnelle**

25.8.1. *Sécurité des micro-ordinateurs et ordinateurs individuels*

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.

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).

25.8.2. *Utilisation de matériel TI personnel pour un travail officiel dans le cadre de la Commission*

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.

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 écrite du ►**M2** directeur de la direction de la sécurité de la Commission ◄. Cette autorisation ne peut être accordée que pour des motifs techniques dans des cas exceptionnels.

▼B

25.8.3. *Utilisation de matériel TI appartenant à un contractant ou fourni par un pays pour un travail officiel dans le cadre de la Commission*

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 de la Commission peut être autorisée par le ►**M2** directeur de la direction de la sécurité de la Commission ◄. L'utilisation 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 de la Commission. 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.

26. COMMUNICATION D'INFORMATIONS CLASSIFIÉES DE L'UE À DES PAYS TIERS OU À DES ORGANISATIONS INTERNATIONALES

26.1.1. *Principes régissant la communication d'informations classifiées de l'UE*

Le collège des membres de la Commission décide d'autoriser la communication d'informations classifiées de l'UE à des pays tiers ou à des organisations internationales 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 la personne à l'origine des informations classifiées de l'UE à communiquer est sollicité.

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 groupe consultatif sur la politique de sécurité de la Commission fournit à la Commission un avis technique sur ce point.

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 la Commission.

26.1.2. *Les niveaux*

Lorsque la Commission décide que des informations classifiées peuvent être communiquées à tel État ou telle organisation internationale ou échangées avec eux, elle fixe 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.

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.

▼B

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.

Chaque niveau de coopération détermine les procédures et les dispositions de sécurité applicables, détaillées aux annexes 3, 4 et 5.

26.1.3. *Accords de sécurité*

Lorsque la Commission décide qu'il y a un besoin permanent ou durable d'échange d'informations classifiées entre la Commission et des États tiers ou d'autres organisations internationales, elle 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.

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.

Les projets d'accords sur les procédures de sécurité ou de mémorandums d'entente sont discutés par le groupe consultatif sur la politique de sécurité de la Commission avant d'être présentés à la Commission pour décision.

Le membre de la Commission chargé des questions de sécurité demande toute l'aide nécessaire aux ANS des États membres pour s'assurer que les informations communiquées sont utilisées et protégées conformément aux termes des accords sur les procédures de sécurité ou des mémorandums d'entente.

▼M3

27. NORMES MINIMALES COMMUNES EN MATIÈRE DE SÉCURITÉ INDUSTRIELLE

27.1 **Introduction**

La présente section traite des aspects liés à la sécurité des activités industrielles qui sont propres à la négociation et à l'attribution de contrats ou de conventions de subvention ainsi qu'à l'exécution par des entités, industrielles ou autres, de ces contrats ou conventions de subvention, dans le cadre desquels sont assignées des tâches qui font intervenir, nécessitent et/ou comportent des informations classifiées de l'UE, y compris la communication de telles informations ou l'accès à celles-ci au cours des procédures de passation des marchés et d'appels à propositions (période de soumission et négociations précontractuelles).

27.2 **Définitions**

Aux fins de ces normes minimales communes, on entend par:

a) «contrat classifié», tout contrat ou convention de subvention en vue de la fourniture de produits, de l'exécution de travaux, de la mise à disposition de bâtiments ou de la prestation de services, dont l'exécution nécessite ou implique l'accès à des informations classifiées de l'UE ou la production de telles informations;

b) «contrat de sous-traitance classifié», un contrat conclu par un contractant ou par le bénéficiaire d'une subvention avec un autre contractant (c'est-à-dire le sous-traitant) en vue de la fourniture de biens, de l'exécution de travaux, de la mise à disposition de bâtiments ou de la prestation de services, dont l'exécution nécessite ou implique l'accès à des informations classifiées de l'UE ou la production de telles informations;

c) «contractant», un opérateur économique ou une entité juridique dotés de la capacité juridique de conclure des contrats ou d'être le bénéficiaire d'une subvention;

▼M3

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

e) «habilitation de sécurité d'installation (HSI)», une décision administrative prise par une ANS ou une ASD selon laquelle, du point de vue de la sécurité, une installation peut assurer de manière suffisante la protection d'informations classifiées de l'UE d'un niveau de classification de sécurité déterminé, et selon laquelle le personnel de l'installation qui doit accéder à des informations classifiées de l'UE possède une habilitation de sécurité appropriée et a été informé des exigences de sécurité nécessaires pour accéder à des informations classifiées de l'UE et les protéger;

f) «entité industrielle ou autre», un contractant ou sous-traitant engagé dans la fourniture de biens, l'exécution de travaux ou la prestation de services, ce qui peut impliquer une entité industrielle, commerciale ou scientifique, ou une entité de service, de recherche, d'enseignement ou de développement;

g) «sécurité industrielle», l'application de mesures et de procédures de protection visant à prévenir, à déceler et à pallier la perte ou la compromission d'informations classifiées de l'UE traitées par un contractant ou un sous-traitant dans le cadre de négociations (pré)contractuelles et de contrats classifiés;

h) «autorité nationale de sécurité (ANS)», l'autorité gouvernementale d'un État membre de l'UE, responsable en dernier ressort de la protection des informations classifiées de l'UE dans cet État membre;

i) «niveau général de classification de sécurité d'un contrat», la détermination de la classification de sécurité de l'ensemble du contrat ou de la convention de subvention, fondée sur la classification d'informations et/ou de matériel qui doivent, ou peuvent, être produits ou communiqués ou auxquels on doit, ou peut, avoir accès au titre de l'un quelconque des éléments du contrat global ou de la convention de subvention globale. Le niveau général de classification de sécurité d'un contrat ne peut être inférieur à la classification la plus élevée de l'un de ses éléments, mais il peut être plus élevé du fait de l'effet d'accumulation;

j) «annexe de sécurité (AS)», un ensemble de conditions contractuelles spéciales, établi par l'autorité contractante, qui fait partie intégrante d'un contrat classifié impliquant l'accès à des informations classifiées de l'UE ou la production de telles informations, dans lequel sont définis les exigences de sécurité ou les éléments du contrat classifié qui doivent être protégés pour des raisons de sécurité;

k) «guide de classification de sécurité (GCS)», un document qui décrit les éléments d'un programme, d'un contrat ou d'une convention de subvention qui sont classifiés et précise les niveaux de classification de sécurité applicables. Le GCS peut être étoffé tout au long de la durée du programme, du contrat ou de la convention de subvention, et les éléments d'information peuvent être reclassifiés ou déclassés. Le GCS doit faire partie de l'AS.

27.3 **Organisation**

a) La Commission peut, par voie de contrat classifié, confier à des entités industrielles ou autres immatriculées dans un État membre des tâches qui font intervenir, nécessitent et/ou comportent des informations classifiées de l'UE.

b) La Commission veille à ce que toutes les exigences découlant des présentes normes minimales soient respectées lors de l'octroi de contrats classifiés.

c) La Commission associe l'ANS ou les ANS compétentes pour appliquer les présentes normes minimales en matière de sécurité industrielle. Les ANS peuvent attribuer ces tâches à une ou plusieurs ASD.

▼M3

d) La responsabilité de la protection des informations classifiées de l'UE au sein des entités industrielles ou autres incombe en dernier ressort à la direction de ces dernières.

e) Chaque fois qu'un contrat ou un contrat de sous-traitance classifié relevant du champ d'application des présentes normes minimales est octroyé, la Commission et/ou l'ANS/ASD, selon le cas, le notifiera rapidement à l'ANS/ASD de l'État membre dans lequel le contractant ou le sous-traitant est immatriculé.

27.4 **Contrats classifiés et décisions d'octroi**

a) La classification de sécurité des contrats ou des conventions de subvention classifiés doit tenir compte des principes suivants:

— la Commission détermine, le cas échéant, les aspects du contrat classifié qui nécessitent une protection et la classification de sécurité appropriée; ce faisant, elle doit tenir compte de la classification de sécurité initiale attribuée par l'autorité d'origine à l'information créée avant l'octroi du contrat classifié,

— le niveau général de classification du contrat ne peut pas être inférieur à la classification la plus élevée de l'un de ses éléments,

— les informations classifiées de l'UE créées dans le cadre d'activités contractuelles sont classifiées conformément au guide de classification de sécurité,

— le cas échéant, la Commission est chargée de modifier le niveau général de classification du contrat ou la classification de sécurité d'un de ses éléments, en consultation avec l'autorité d'origine, et d'en informer toutes les parties intéressées,

— les informations classifiées communiquées au contractant ou au sous-traitant ou créées dans le cadre d'une activité contractuelle ne doivent pas être utilisées à d'autres fins que celles prévues par le contrat classifié et ne doivent pas être divulguées à des tiers sans le consentement écrit préalable de l'autorité d'origine.

b) La Commission et les ANS/ASD des États membres concernés sont chargées de veiller à ce que les contractants et les sous-traitants à qui sont octroyés des contrats classifiés faisant intervenir des informations classifiées CONFIDENTIEL UE ou au-delà prennent toutes les mesures appropriées pour protéger les informations de ce type qui leur sont communiquées ou qu'ils créent lors de l'exécution du contrat classifié conformément aux législations et aux réglementations nationales. Le non-respect des exigences de sécurité peut entraîner la résiliation du contrat classifié.

c) Toutes les entités industrielles ou autres participant à des contrats classifiés qui impliquent l'accès à des informations classifiées CONFIDENTIEL UE ou au-delà doivent être en possession d'une HSI nationale. Cette habilitation est délivrée par l'ANS/ASD de l'État membre pour confirmer qu'une installation peut assurer et garantir aux informations classifiées de l'UE la protection de sécurité adéquate au niveau de classification approprié.

d) Lorsqu'un contrat classifié est accordé, un responsable de la sécurité d'installation (RSI), désigné par la direction du contractant ou du sous-traitant, est chargé de demander une habilitation de sécurité du personnel (HSP) pour toutes les personnes employées dans des entités industrielles ou autres immatriculées dans un État membre et dont les fonctions nécessitent qu'elles aient accès à des informations classifiées CONFIDENTIEL UE ou au-delà faisant l'objet d'un contrat classifié; cette habilitation est délivrée par l'ANS/ASD de l'État membre conformément à sa réglementation nationale.

▼**M3**

e) Les contrats classifiés doivent inclure l'AS telle que définie au point 27.2, j). L'AS doit contenir le GCS.

f) Avant de lancer une procédure négociée pour un contrat classifié, la Commission contactera l'ANS/ASD de l'État membre dans lequel les entités industrielles ou autres concernées sont immatriculées afin d'obtenir la confirmation qu'elles sont en possession d'une HSI en cours de validité et adaptée au niveau de classification de sécurité du contrat.

g) L'autorité contractante ne doit pas attribuer un contrat classifié à l'opérateur économique sélectionné avant d'avoir reçu le certificat de HSI en cours de validité.

h) Sauf si les législations et réglementations nationales des États membres l'imposent, une HSI n'est pas nécessaire pour les contrats faisant intervenir des informations classifiées RESTREINT UE.

i) Les appels d'offres concernant des contrats classifiés doivent contenir une disposition prévoyant qu'un opérateur économique qui ne présente pas d'offre ou qui n'est pas sélectionné sera tenu de restituer tous les documents dans un délai spécifié.

j) Il se peut que les contractants doivent négocier des contrats de sous-traitance classifiés avec des sous-traitants à différents niveaux. Le contractant est chargé de veiller à ce que toutes les activités de sous-traitance soient menées conformément aux normes minimales communes énoncées dans la présente section. Il ne doit toutefois pas transmettre d'informations ou de matériel classifiés de l'UE à un sous-traitant sans le consentement écrit préalable de l'autorité d'origine.

k) Les conditions dans lesquelles un contractant peut sous-traiter des activités doivent être définies dans l'appel d'offres ou dans l'appel à propositions, ainsi que dans le contrat classifié. Aucun contrat de sous-traitance ne peut être accordé à des entités immatriculées dans un État non membre de l'UE sans l'autorisation écrite expresse de la Commission.

l) Pendant toute la durée du contrat classifié, le respect de toutes les dispositions en matière de sécurité y figurant sera supervisé conjointement par la Commission et l'ANS/ASD compétente. Tout incident de sécurité fait l'objet d'un rapport, conformément aux dispositions prévues dans la partie II, section 24, des présentes règles en matière de sécurité. La modification ou le retrait d'une HSI doit immédiatement être communiqué à la Commission et à toute autre ANS/ASD à laquelle elle a été notifiée.

m) Lorsqu'un contrat ou un contrat de sous-traitance classifié est résilié, la Commission et/ou l'ANS/ASD, selon le cas, le notifiera rapidement à l'ANS/ASD de l'État membre dans lequel le contractant ou sous-traitant est immatriculé.

n) Les normes minimales communes figurant dans la présente section continuent à être respectées, et les contractants et sous-traitants maintiennent la confidentialité des informations classifiées après résiliation ou expiration du contrat ou du contrat de sous-traitance classifié.

o) Des dispositions spécifiques pour la destruction des informations classifiées au terme du contrat classifié seront énoncées dans l'AS ou dans d'autres dispositions pertinentes prévoyant des exigences de sécurité.

p) Les obligations et conditions visées dans la présente section s'appliquent mutatis mutandis aux procédures d'octroi de subventions par voie de décision, et notamment aux bénéficiaires de ces subventions. La décision d'octroi énonce l'ensemble des obligations des bénéficiaires.

▼M3

27.5 **Visites**

Lorsque le personnel de la Commission visite, dans le cadre de contrats classifiés, des entités industrielles ou autres des États membres chargées d'exécuter des contrats classifiés de l'UE, ces visites doivent être organisées avec l'ANS/ASD compétente. Les visites effectuées par des employés des entités industrielles ou autres dans le cadre d'un contrat classifié de l'UE doivent être organisées par les ANS/ASD concernées. Les ANS/ASD associées à un contrat classifié de l'UE peuvent toutefois convenir d'une procédure prévoyant que les visites effectuées par des employés des entités industrielles ou autres puissent être organisées directement.

27.6 **Transmission et transport d'informations classifiées de l'UE**

a) En ce qui concerne la transmission d'informations classifiées de l'UE, les dispositions figurant dans la partie II, section 21, des présentes règles en matière de sécurité s'appliquent. Afin de compléter ces dispositions, toutes les procédures existantes en vigueur entre les États membres s'appliqueront.

b) Le transport international de matériel classifié de l'UE relatif à des contrats classifiés s'effectue conformément aux procédures nationales des États membres. Les principes suivants seront appliqués lors de l'examen des arrangements en matière de sécurité pour le transport international:

   — la sécurité est assurée à chaque étape du transport et en toutes circonstances, du point d'origine jusqu'à la destination finale,

   — le degré de protection attribué à un lot est déterminé en fonction du niveau de classification le plus élevé du matériel qu'il contient,

   — une HSI est obtenue, le cas échéant, pour des sociétés assurant le transport. Dans ce cas, le personnel qui manipule le lot doit recevoir une habilitation de sécurité conformément aux normes minimales communes figurant dans la présente section,

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

   — il est préférable, à chaque fois que c'est possible, que les itinéraires ne traversent que des États membres de l'UE. Les itinéraires traversant des États non membres de l'UE ne doivent être empruntés qu'avec l'autorisation de l'ANS/ASD de l'État de l'expéditeur et de celui du destinataire,

   — avant tout transfert de matériel classifié de l'UE, un plan de transport est élaboré par l'expéditeur et approuvé par les ANS/ASD concernées.

▼M1

Appendice 1

COMPARAISON ENTRE LES CLASSIFICATIONS DE SÉCURITÉ NATIONALES

Classification UE	TRES SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Classification UEO	FOCAL TOP SECRET	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Classification Euratom	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Classification OTAN	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
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 ([1]) — Vertraulich	VS — Nur für den Dienstgebrauch
Grèce	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Espagne	Secreto	Reservado	Confidencial	Difusión Limitada
France	Très Secret Défense ([2])	Secret Défense	Confidentiel Défense	

▼M4

Croatie	Vrlo tajno	Tajno	Povjerljivo	Ograničeno

▼M1

Irlande	Top Secret	Secret	Confidential	Restricted
Italie	Segretissimo	Segreto	Riservatissimo	Riservato
Luxembourg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Pays-Bas	Stg ([3]). Zeer Geheim	Stg. Geheim	Stg. Confidentieel	Departementaal-vertrouwelijk
Autriche	Streng Geheim	Geheim	Vertraulich	Eingeschränkt

▼**M1**

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
Chypre	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
Estonie	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Hongrie	Szigorúan titkos !	Titkos !	Bizalmas !	Korlátozott terjesztésű !
Lettonie	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lituanie	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Malte	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Pologne	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
République tchèque	Přísn tajné	Tajné	Důvěrné	Vyhrazené
Slovaquie	Prísne tajné	Tajné	Dôverné	Vyhradené
Slovénie	Strogo tajno	Tajno	Zaupno	SVN Interno

([1]) VS = Verschlusssache.
([2]) La classification Très secret défense, couvrant les priorités gouvernementales, ne peut s'échanger qu'avec l'autorisation du premier ministre.
([3]) Stg = staatsgeheim.

▼B

Appendice 2

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 16, 17, 20 et 21.

Classification	Quand	Qui	Apposition des classifications et des timbres	Déclassement/déclassification/destruction	
				Qui	Quand
►**M1** TRES 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 [16.1].	La compromission d'informations ou de matériels classifiés ►**M1** TRES 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.	Personnes dûment autorisées (autorités d'origine), directeurs généraux, chefs de service [17.1] Les autorités d'origine fixent une date, un délai ou un événement à partir duquel les informations contenues dans un document pourront être déclassées ou déclassifiées [16.2]. Sinon, elles réexaminent la question tous les cinq ans au plus pour s'assurer que la classification initiale reste nécessaire [17.3].	La classification ►**M1** TRES SECRET UE/EU TOP SECRET ◄ est apposée sur les documents ►**M1** TRES SECRET UE/EU TOP SECRET ◄, le cas échéant avec un identifiant de sécurité et/ou le timbre défense PESD, par voie mécanique et à la main [16.4, 16.5, 16.3]. Les classifications UE et identifiants de sécurité 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 [21.1].	La décision de déclassifier ou de déclasser un document revient exclusivement à l'autorité d'origine, qui doit informer du changement de classification les destinataires successifs auxquels elle a fait suivre l'original ou une copie du document [17.3]. Les document ►**M1** TRES SECRET UE/EU TOP SECRET ◄ sont détruits par le bureau d'ordre central ou subordonné qui en a la charge. Chaque document détruit est inscrit sur un procès-verbal de destruction, signé par l'officier contrôleur ►**M1** TRES SECRET UE/EU TOP SECRET ◄ et par un témoin, qui doit être habilité ►**M1** TRES SECRET UE/EU TOP SECRET ◄. Le cahier d'enregistrement doit comporter une note à cet effet. Le bureau d'ordre doit conserver pendant dix ans les procès-verbaux de destruction ainsi que les fiches de circulation [22.5].	Les exemplaires excédentaires et les documents jugés périmés doivent être détruits [22.5]. Les documents ►**M1** TRES SECRET UE/EU TOP SECRET ◄, y compris tous les rebuts classifiés résultant de l'élaboration des documents ►**M1** TRES SECRET UE/EU TOP SECRET ◄ (exemplaires endommagés, brouillons, notes dactylographiées, papiers carbones, etc.), doivent être détruits, sous la surveillance d'un officier de contrôle ►**M1** TRES SECRET UE/EU TOP SECRET ◄, par incinération, réduction en pulpe, lacération en bandes ou division en fragments non identifiables rendant impossible toute reconstitution [22.5].

Classification	Quand	Qui	Apposition des classifications et des 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 [16.1].	La compromission d'informations ou de matériels classifiés 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'efficiacité d'opérations de sécurité ou de renseignements 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.	Personnes autorisées (autorités d'origine), directeurs généraux, chefs de service [17.1]. Les autorités d'origine fixent une date, un délai à partir duquel les informations contenues dans un document pourront être déclassées ou déclassifiées [16.2]. Sinon, elles réexaminent la question tous les cinq ans au plus pour s'assurer que la classification initiale reste nécessaire [17.3].	La classification SECRET UE est apposée sur les documents SECRET UE, le cas échéant avec un indentifiant de sécurité et/ou le timbre défense PESD, par voie mécanique et à la main [16.4, 16.5, 16.3]. Les classifications UE et identifiants de sécurité 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 [21.1].	La décision de déclassifier ou de déclasser un document revient exclusivement à l'autorité d'origine, qui doit informer du changement de classification les destinataires successifs auxquels elle a fait suivre l'original ou une copie du document [17.3]. 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 inscits 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 [22.5].	Les exemplaires excédentaires et les documents jugés périmés doivent être détuits [22.5]. 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 [22.5].
CONFIDENTIEL UE:	La compromission d'informations ou de matériels classifiés CONFIDENTIEL UE risquerait de: — causer un préjudice important aux relations diplomatiques, c'est-à-dire donner lieu à des protestations officielles ou autres sanctions	Personnes autorisées (autorités d'origine), directeurs généraux, chefs de service [17.1].	La classification CONFIDENTIEL UE est apposée sur les documents CONFIDENTIEL UE et entraîne, le cas échéant, l'apposition d'un identifiant de sécurité et/ou du timbre défense PESD, par voie mécanique et à la main ou par impression sur du papier portant un cachet préimprimé et enregistré [16.4, 16.5, 16.3].	La décision de déclassifier ou de déclasser un document revient exclusivement à l'autorité d'origine, qui doit informer du changement de classification les destinataires successifs auxquels elle a fait suivre l'original ou une copie du document [17.3].	Les exemplaires excédentaires et les documents jugés périmés doivent être détruits [22.5].

▼B

Classification	Quand	Qui	Apposition des classifications et des timbres	Déclassement/déclassification/destruction	
				Qui	Quand
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 [16.1].	— 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 renseignements 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.	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 [17.3].	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 [21.1].	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 de la Commission ou d'organismes décentralisés de l'UE, conformément aux instructions du ►**M2** membre de la Commission chargé des questions de sécurité ◄ [22.5].	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 toutes reconstitution [22.5].

▼B

Classification	Quand	Qui	Apposition des classifications et des timbres	Déclassement/déclassification/destruction	
				Qui	Quand
►M1 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 plusieurs de ses États membres [16.1].	La compromission d'informations ou de matériels classés 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	Personnes autorisées (autorité d'origine), directeurs généraux, chefs de service [17.1]. Les autorités d'origine fixent une date, un délai ou un événement à partir duquel les informations contenues dans un document pourront être déclassées ou déclassifiées [16.2]. Sinon, elles réexaminent la question tous les cinq ans au plus pour s'assurer que la classification initiale reste nécessaire [17.3].	La classification RESTREINT UE sera apposée sur les documents RESTREINT UE, le cas échéant avec un identifiant de sécurité et/ou le timbre défense PESD, par voie mécanique ou électronique [16.4, 16.5 et 16.3]. La classification et les identifiants de sécurité UE doivent apparaître en haut de la première page et chaque page doit être numérotée. Chaque document doit porter un numéro de référence ainsi qu'une date [21.1].	La décision de déclassifier un document revient exclusivement à l'autorité d'origine, qui doit informer du changement de classification les destinataires successifs auxquels elle a fait suivre l'original ou une copie du document [17.3]. Les documents RESTREINT UE sont détruits par le bureau d'ordre qui en a la charge ou par l'utilisateur, conformément aux intructions du ►M2 membre de la Commission chargé des questions de sécurité ◄ [22.5].	Les exemplaires excédentaires et les documents jugés périmés doivent être détruits [22.5].

▼B

Appendice 3

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 de la Commission en tant que Collège.

2. Sous réserve de la conclusion d'un accord de sécurité, il est du ressort du membre de la Commission chargé des questions de sécurité d'examiner les demandes de communication d'informations classifiées de l'UE.

3. À ce titre, il lui incombe:

   — de recueillir l'avis des autorités d'origine des informations classifiées à communiquer,

   — d'établir 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 aux présentes règles de sécurité,

   — de recueillir l'avis du groupe consultatif de la Commission sur la politique de sécurité sur la confiance que l'on peut accorder aux pays ou organismes internationaux bénéficiaires.

4. Le membre de la Commission chargé des questions de sécurité transmet pour décision à la Commission la demande et l'avis rendu par le groupe consultatif de la Commission sur la politique de sécurité.

RÈGLES DE SÉCURITÉ À APPLIQUER PAR LES BÉNÉFICIAIRES

5. La décision de la Commission d'autoriser la communication d'informations classifiées de l'UE est portée à la connaissance des États ou des organisations internationales bénéficiaires par le membre de la Commission chargé des questions de sécurité.

6. 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,

   — a les protéger conformément aux présentes règles en matière de sécurité et notamment aux règles 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. Sous réserve de la conclusion d'un tel accord, les dispositions de la section 21 s'appliquent. L'accord précise en particulier à quels bureaux d'ordre sont transmises les informations classifiées UE.

▼B

b) Si la communication d'informations classifiées de l'UE autorisée par la Commission 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 XXII des présentes règles 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 22 des présentes règles 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 à la ►**M2** direction de la sécurité de la Commission ◄.

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 la ►**M2** direction de la sécurité de la Commission ◄, les 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 de la ►**M2** direction de la sécurité de la Commission ◄ propre à empêcher une récidive.

▼B

14. Inspections

La ►M2 direction de la sécurité de la Commission ◄ est autorisée 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 les présentes règles de sécurité sont respectées.

▼B

Appendice 4

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 de l'autorité d'origine. La communication d'informations classifiées de l'UE créées au sein de la Commission est du ressort de la Commission en tant que Collège.

2. Elle est, en principe, limitée aux informations classifiées jusqu'au niveau SECRET UE inclus; en sont exclues, les informations classifiées protégées par des codes ou des timbres de sécurité spéciaux.

3. Sous réserve de la conclusion d'un accord de sécurité, il est du ressort du membre de la Commission chargé des questions de sécurité d'examiner les demandes de communication d'informations classifiées UE.

4. À ce titre, il lui incombe:

   — de recueillir l'avis des autorités d'origine des informations classifiées UE à communiquer,

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

   — d'organiser une réunion du groupe consultatif de la Commission sur la politique de sécurité ou d'interroger, par procédure de silence le cas échéant, les autorités nationales de sécurité des États membres en vue de recueillir l'avis du groupe consultatif de la Commission sur la politique de sécurité.

5. L'avis du groupe consultatif de la Commission sur la politique de sécurité 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.

6. Le membre de la Commission chargé des questions de sécurité transmet à la Commission pour décision la demande et l'avis rendu par le groupe consultatif de la Commission sur la politique de sécurité.

RÈGLES DE SÉCURITÉ À APPLIQUER PAR LES BÉNÉFICIAIRES

7. La décision de la Commission d'autoriser la communication d'informations classifiées de l'UE et de ses restrictions est portée à la connaissance des États ou des organisations internationales bénéficiaires par le membre de la Commission chargé des questions de sécurité.

▼B

8. 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 la Commission.

9. 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 la Commission sur avis technique du groupe consultatif de la Commission sur la politique de sécurité.

10. 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 ►M2 directeur de la direction de la sécurité de la Commission ◄.

11. Transmission des documents

Les modalités pratiques de transmission des documents sont arrêtées en commun. Sous réserve de la conclusion d'un tel accord, les dispositions de la section 21 s'appliquent. L'accord indique 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.

12. 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.

13. Renvoi des documents

Lorsque le destinataire renvoie un document classifié à la Commission ou à l'État membre qui l'a communiqué, il procède comme indiqué au paragraphe précité «Transmission des documents».

14. 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

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 de la ►M2 direction de la sécurité de la Commission ◄.

d) Il convient de définir et de confirmer avec la ►M2 direction de la sécurité de la Commission ◄ la procédure à suivre pour la destruction rapide et totale des documents en cas d'urgence.

15. 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.

16. 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 à la ►M2 direction de la sécurité de la Commission ◄ ou à l'ANS de l'État membre ayant pris l'initiative de communiquer les documents (avec copie à la ►M2 direction de la sécurité de la Commission ◄);

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.

17. Inspections

La ►M2 direction de la sécurité de la Commission ◄ est autorisée 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.

18. Rapports

Sous réserve la conclusion d'un accord de sécurité, tant que l'État ou l'organisation détient des informations classifiées de l'UE, elle doit soumettre chaque année, à une date fixée lorsque l'autorisation lui est donnée de recevoir ces informations, un rapport confirmant que les présentes règles de sécurité sont respectées.

▼B

Appendice 5

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 la Commission décide de coopérer, dans certaines circonstances particulières, avec des États ou des organisations ne pouvant fournir les garanties exigées aux termes des présentes règles de sécurité: une telle coopération peut pourtant nécessiter la communication d'informations classifiées de l'UE.

2. 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 de l'autorité d'origine. La communication d'informations classifiées de l'UE créées au sein de la Commission est du ressort de la Commission en tant que Collège.

   Elle est, en principe, limitée aux informations classifiées jusqu'au niveau SECRET UE inclus; en sont exclues, les informations classifiées protégées par des codes ou des timbres de sécurité spéciaux.

3. La Commission 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.

4. Si la Commission émet un avis favorable, il incombe au membre de la Commission chargé des questions de sécurité:

   — de recueillir les avis des autorités d'origine des informations classifiées de l'UE à communiquer,

   — d'organiser une réunion avec le groupe consultatif de la Commission sur la politique de sécurité ou d'interroger, par procédure de silence le cas échéant, les autorités nationales de sécurité des États membres en vue de recueillir l'avis du groupe consultatif de la Commission sur la politique de sécurité.

5. L'avis du groupe consultatif de la Commission sur la politique de sécurité 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;

   c) déclassement ou déclassification préalable avant communication de l'information;

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

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

6. 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 groupe consultatif de la Commission sur la politique de sécurité 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.

▼B

7. Le ►M2 membre de la Commission chargé des questions de sécurité ◄ transmet à la Commission pour décision l'avis du groupe consultatif de la Commission sur la politique de sécurité.

8. Dès que la communication d'informations classifiées de l'UE et que les modalités pratiques d'exécution sont approuvées par la Commission, la ►M2 direction de la sécurité de la Commission ◄ 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.

9. Le membre de la Commission chargé des questions de sécurité informe les États membres de la nature et de la classification des informations, en établissant la liste des organisations et des pays auxquels elles peuvent être communiquées, selon les décisions de la Commission.

10. La ►M2 direction de la sécurité de la Commission ◄ prend toute mesure nécessaire pour faciliter l'évaluation du dommage et les révisions de procédures ultérieures éventuelles.

La Commission réexamine la question, chaque fois que les conditions de coopération sont modifiées.

RÈGLES DE SÉCURITÉ À APPLIQUER PAR LES BÉNÉFICIAIRES

11. Le membre de la Commission chargé des questions de sécurité notifie aux États ou organisations internationales bénéficiaires la décision de la Commission d'autoriser la communication d'informations classifiées de l'UE, accompagnée des règles de protection détaillées proposées par le groupe consultatif de la Commission sur la politique de sécurité et approuvées par la Commission.

12. 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 la Commission,

— à leur assurer la protection exigée par la Commission.

13. Transmission des documents

a) Les modalités pratiques de transmission des documents sont arrêtées en commun entre la ►M2 direction de la sécurité de la Commission ◄ 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 récépissé 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.

▼B

14. 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.

15. 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 verrouillées 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.

16. 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.

17. 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. La ►M2 direction de la sécurité de la Commission ◄ est informée de ses résultats. 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.

▼B

Appendice 6

LISTE DES ABRÉVIATIONS

CrA	Autorité Crypto
CCAM	Commission Consultative des Achats et Marchés
CISO	Responsable de la sécurité informatique au niveau central
COMPUSEC	Sécurité informatique
COMSEC	Sécurité des communications
CSO	►M2 Direction de la sécurité de la Commission ◄
ESDP	Politique européenne de sécurité et de défense
EUPSC	Habilitation de sécurité de l'UE
IA	Service INFOSEC
INFOSEC	Sécurité de l'information
IO	Propriétaire de l'information
ISO	Organisation internationale de normalisation
IT	Technologie de l'information
LISO	Responsable de la sécurité informatique au niveau local
LSO	Responsable local de la sécurité
MSO	Responsable de la sécurité de la réunion
NSA	Autorité nationale de sécurité
PC	Ordinateur personnel
RCO	Agent contrôleur
SAA	Autorité d'homologation de sécurité
SecOP	Procédures opérationnelles en matière de sécurité
SSRS	Prescriptions en matière de sécurité
TA	Autorité TEMPEST
TSO	Autorité d'exploitation des systèmes techniques

▼M3

ASD	Autorité de sécurité désignée
HSI	Habilitation de sécurité d'installation
RSI	Responsable de la sécurité d'installation
HSP	Habilitation de sécurité du personnel
AS	Annexe de sécurité
GCS	Guide de classification de sécurité.