DÉCISION (UE) 2022/640 DE LA COMMISSION

du 7 avril 2022

établissant les modalités d'application des rôles et responsabilités des principaux acteurs de la sécurité

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 249,

vu la décision (UE, Euratom) 2015/443 de la Commission du 13 mars 2015 relative à la sécurité au sein de la Commission ([1]),

vu la décision (UE, Euratom) 2015/444 de la Commission du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne ([2]),

considérant ce qui suit:

(1) Les décisions (UE, Euratom) 2015/443 et (UE, Euratom) 2015/444 s'appliquent à tous les départements et locaux de la Commission.

(2) Le cas échéant, les modalités d'application en complément ou à l'appui de la décision (UE, Euratom) 2015/444 doivent être adoptées conformément à son article 60.

(3) Les mesures de sécurité pour la protection des informations classifiées de l'Union européenne tout au long de leur cycle de vie devraient être proportionnées en particulier à leur classification de sécurité.

(4) Les mesures de sécurité pour la protection des systèmes d'information et de communication au sein de la Commission sont définies dans la décision (UE, Euratom) 2017/46 de la Commission ([3]), en particulier à l'article 3 relatif aux principes de sécurité informatique au sein de la Commission et à l'article 9 relatif aux propriétaires de systèmes.

(5) L'objectif des modalités d'application relatives aux rôles et responsabilités des principaux acteurs de la sécurité est de fournir des orientations sur les conditions préalables et les tâches qui sont définies pour ces rôles dans les décisions (UE, Euratom) 2015/443 et (UE, Euratom) 2015/444.

(6) L'article 36, paragraphe 7, de la décision (UE, Euratom) 2015/444 prévoit un certain nombre de fonctions supplémentaires liées à la sécurité que l'autorité de sécurité de la Commission doit exercer. Les tâches liées à ces fonctions sont définies dans la présente décision.

(7) Les responsables locaux de la sécurité (LSO) et les agents contrôleurs (RCO) ont des responsabilités spécifiques en matière de protection des informations classifiées de l'UE dans leurs départements, conformément à la décision (UE, Euratom) 2015/444.

(8) Le 4 mai 2016, la Commission a adopté une décision ([4]) qui habilite le membre de la Commission chargé des questions de sécurité à adopter, au nom de la Commission et sous sa responsabilité, les modalités d'application prévues par l'article 60 de la décision (UE, Euratom) 2015/444; par la suite, le 13 avril 2021, le membre de la Commission chargé des questions de sécurité a adopté, au nom et sous la responsabilité de la Commission, une décision ([5]) portant subdélégation desdites modalités d'application au directeur général de la direction générale Ressources humaines et sécurité,

([1]) JO L 72 du 17.3.2015, p. 41.
([2]) JO L 72 du 17.3.2015, p. 53.
([3]) Décision (UE, Euratom) 2017/46 de la Commission du 10 janvier 2017 sur la sécurité des systèmes d'information et de communication au sein de la Commission européenne (JO L 6 du 11.1.2017, p. 40).
([4]) Décision C(2016) 2797 de la Commission du 4 mai 2016 relative à une habilitation en matière de sécurité.
([5]) Décision C(2021) 2684 de la Commission du 13 avril 2021 accordant une subdélégation de pouvoirs conférée par la décision C(2016) 2797 de la Commission relative à une habilitation en matière de sécurité.

A ADOPTÉ LA PRÉSENTE DÉCISION:

CHAPITRE 1

Dispositions générales

Article premier

Objet et champ d'application

1. La présente décision définit les rôles et responsabilités des principaux acteurs de la sécurité qui sont chargés de la protection des informations classifiées de l'UE (ICUE) au sein de la Commission au titre des décisions (UE, Euratom) 2015/443 et (UE, Euratom) 2015/444.

2. La présente décision s'applique à tous les départements de la Commission et dans l'ensemble des locaux de la Commission.

CHAPITRE 2

Direction générale Ressources humaines et sécurité

Article 2

Autorité de sécurité de la Commission

1. Le directeur de la direction Sécurité au sein de la direction générale Ressources humaines et sécurité est l'autorité de sécurité de la Commission visée à l'article 7 de la décision (UE, Euratom) 2015/444.

2. L'autorité de sécurité de la Commission exerce ses fonctions dans les domaines ci-après ainsi que prévu par la décision (UE, Euratom) 2015/444, conformément aux articles 3 à 7 de la présente décision:

a) la sécurité du personnel;

b) la sécurité physique;

c) la gestion des ICUE;

d) l'homologation de tout système d'information et de communication (SIC) traitant des ICUE;

e) la sécurité industrielle; et

f) l'échange d'informations classifiées.

3. L'autorité de sécurité de la Commission assure la formation obligatoire des responsables locaux de la sécurité (LSO), des LSO adjoints, des agents contrôleurs (RCO) et des RCO adjoints au sujet de leurs responsabilités et fonctions.

Article 3

Autorité chargée de l'assurance de l'information

L'autorité chargée de l'assurance de l'information est responsable des activités suivantes en rapport avec la protection des ICUE:

a) élaborer des politiques relatives à l'assurance de l'information et des lignes directrices en matière de sécurité et contrôler leur efficacité et leur pertinence;

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

c) veiller à ce que les mesures d'assurance de l'information soient conformes aux politiques de sécurité et de passation de marchés de la Commission, le cas échéant;

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

e) consulter les propriétaires de systèmes, les fournisseurs de systèmes, les acteurs de la sécurité et les représentants des utilisateurs en ce qui concerne les politiques relatives à l'assurance de l'information et les lignes directrices en matière de sécurité.

Article 4

Autorité d'homologation de sécurité

1. L'autorité de sécurité de la Commission est chargée de l'homologation des zones sécurisées qui satisfont aux exigences de l'article 18 de la décision 2015/444 et des SIC pour le traitement des ICUE.

2. Les départements de la Commission consultent l'autorité d'homologation de sécurité (AHS) en coordination avec leur LSO et leur LISO, le cas échéant, chaque fois qu'un département a l'intention:

a) de construire une zone sécurisée;

b) de mettre en œuvre un SIC pour traiter des ICUE;

c) d'installer tout autre équipement pour le traitement des informations classifiées, y compris les connexions avec un SIC tiers.

L'autorité d'homologation de sécurité fournit des conseils sur ces activités au cours des processus tant de planification que de construction ou de développement.

3. Les ICUE ne sont pas traitées dans une zone sécurisée ou un SIC avant que l'autorité d'homologation de sécurité n'ait délivré une homologation au niveau approprié d'ICUE.

4. Les exigences relatives à l'homologation d'une zone sécurisée portent notamment sur:

a) l'approbation des plans pour la zone sécurisée;

b) l'approbation d'éventuels marchés de travaux exécutés par des contractants externes, en tenant compte des dispositions en matière de sécurité industrielle, telles que les éventuelles exigences en matière d'habilitations de sécurité des contractants et de leur personnel;

c) la disponibilité de toutes les déclarations et certificats de conformité requis;

d) une inspection physique de la zone sécurisée afin de vérifier que les matériaux et méthodes de construction, les contrôles d'accès, les équipements de sécurité et tout autre élément sont conformes aux exigences établies par l'autorité de sécurité de la Commission;

e) la validation des contre-mesures destinées à lutter contre les rayonnements électromagnétiques pour toute zone techniquement sécurisée;

f) l'approbation des procédures d'exploitation de sécurité (SecOP) pour la zone sécurisée.

5. Les exigences relatives à l'homologation d'un SIC traitant des ICUE portent notamment sur:

a) la création d'une stratégie d'homologation du système;

b) la validation du plan de sécurité du SIC, sur la base d'une approche de gestion des risques;

c) la validation des SecOP pour le SIC;

d) la validation de tous les autres documents de sécurité requis, tels que déterminés par l'autorité d'homologation de sécurité;

e) l'approbation de toute utilisation de technologies de cryptage;

f) la validation des contre-mesures destinées à lutter contre les rayonnements électromagnétiques pour un SIC traitant des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur;

g) l'inspection du SIC afin de vérifier que les mesures de sécurité documentées sont correctement mises en œuvre.

6. Une fois que les exigences en matière d'homologation sont remplies avec succès, l'autorité d'homologation de sécurité délivre une autorisation formelle pour le traitement des ICUE dans la zone sécurisée ou le SIC, pour un niveau maximal déterminé d'ICUE et pour une durée maximale de 5 ans, en fonction des niveaux d'ICUE traitées et des risques encourus.

7. Dès la notification d'une infraction à la sécurité ou d'une modification importante de la conception ou des mesures de sécurité d'une zone sécurisée ou d'un SIC, l'autorité d'homologation de sécurité réexamine et, si nécessaire, peut révoquer l'autorisation de traiter des ICUE jusqu'à ce que les problèmes identifiés soient résolus.

Article 5

Autorité TEMPEST

1. Des mesures de sécurité TEMPEST sont mises en œuvre pour protéger les SIC traitant des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, et peuvent être mises en œuvre pour les informations classifiées RESTREINT UE/EU RESTRICTED.

2. L'autorité TEMPEST est responsable de l'approbation des mesures adoptées afin d'assurer la protection contre la compromission des ICUE par des émissions électromagnétiques non intentionnelles;

3. À la demande d'un propriétaire d'un SIC traitant des ICUE, l'autorité TEMPEST publie des spécifications pour les mesures de sécurité TEMPEST ainsi qu'il convient pour le niveau de classification des informations.

4. L'autorité TEMPEST effectue des essais techniques au cours de l'homologation des zones sécurisées et des SIC pour le traitement des ICUE au niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur et délivre un certificat TEMPEST lorsque les tests sont concluants.

5. Un certificat TEMPEST précise au moins:

a) la date du test;

b) une description des mesures de sécurité TEMPEST, avec les plans des locaux;

c) la limite de validité du certificat,

d) tout changement susceptible d'invalider la certification;

e) la signature de l'autorité TEMPEST.

6. Un LSO ou un organisateur de réunions chargé d'organiser une réunion classifiée, en coordination avec le LSO, peut demander à l'autorité TEMPEST de tester les salles de réunion afin de s'assurer qu'elles sont techniquement sécurisées.

Article 6

Autorité d'agrément cryptographique

1. L'autorité d'agrément cryptographique est chargée d'approuver l'utilisation des technologies de cryptage.

2. L'autorité d'agrément cryptographique publie des orientations sur les exigences relatives à l'utilisation et à l'approbation des technologies de cryptage.

3. L'autorité d'agrément cryptographique approuve l'utilisation de solutions de cryptage sur la base d'une demande du propriétaire du système. L'agrément est fondé sur une évaluation satisfaisante d'au moins:

a) les besoins de sécurité des informations à protéger;

b) une vue d'ensemble du SIC concerné par la solution;

c) une évaluation des risques inhérents et résiduels;

d) une description de la solution proposée;

e) les SecOP pour la solution de cryptage.

4. L'autorité d'agrément cryptographique tient un registre des solutions de cryptage approuvées.

Article 7

Autorité de distribution cryptographique

1. l'autorité de distribution cryptographique est responsable de la distribution du matériel cryptographique utilisé pour protéger les ICUE (principalement matériel de chiffrement, clés cryptographiques, certificats et authentificateurs connexes):

a) aux utilisateurs ou départements au sein de la Commission pour les SIC gérés par des tiers;

b) aux utilisateurs ou organisations en dehors de la Commission pour les SIC gérés par la Commission.

2. L'autorité de distribution cryptographique peut déléguer la distribution de matériel cryptographique destiné à des tiers à d'autres départements, conformément à l'article 17, paragraphe 3, de la décision 2015/443.

3. L'autorité de distribution cryptographique veille à ce que tout le matériel cryptographique soit envoyé par des canaux sécurisés qui protègent contre toute altération et montrent les signes d'une éventuelle altération, conformément aux règles de sécurité applicables au niveau de classification des ICUE qui seront protégées par ce matériel.

4. L'autorité de distribution cryptographique fournit des orientations au LSO et, le cas échéant, au responsable de la sécurité informatique au niveau local (LISO) de chaque département de la Commission qui participe à la production, à la distribution ou à l'utilisation du matériel cryptographique.

5. L'autorité de distribution cryptographique veille à ce que des SecOP appropriés soient établis pour le processus de distribution.

CHAPITRE 3

Départements de la Commission

Article 8

Chefs de départements

1. Chaque chef de département désigne:

a) un LSO et un ou plusieurs adjoints, le cas échéant, pour chaque département ou cabinet;

b) un RCO et un ou plusieurs adjoints, le cas échéant, pour chaque département qui gère un bureau d'ordre pour les ICUE;

c) un propriétaire de système pour chaque SIC traitant des ICUE.

2. Le chef de département demande l'approbation du directeur de la direction Sécurité au sein de la direction générale Ressources humaines et sécurité avant la désignation des LSO, des LSO adjoints, des RCO et des RCO adjoints.

3. Le chef de département identifie tous les postes nécessitant une habilitation pour accéder aux ICUE, en consultation avec le LSO. Les candidats à de tels postes sont informés de l'obligation d'habilitation au cours de la procédure de recrutement.

4. Le chef de tout département détenant des ICUE est responsable de l'activation des plans de destruction et d'évacuation d'urgence si nécessaire. Ces plans prévoient une solution de remplacement pour les situations dans lesquelles le chef de département ne peut être contacté.

Article 9

Propriétaires de SIC traitant des ICUE

1. Le propriétaire du système contacte l'autorité d'homologation de sécurité le plus tôt possible dans le cadre d'un projet visant à mettre en œuvre un SIC traitant des ICUE afin de déterminer les normes et exigences de sécurité applicables et d'entamer le processus d'homologation de sécurité.

2. Le propriétaire du système veille à ce que les mesures de sécurité soient conformes aux exigences de l'autorité d'homologation de sécurité et à ce que le SIC ne traite pas des ICUE avant d'avoir été homologué.

3. Le propriétaire du système prend contact avec l'autorité d'agrément cryptographique pour obtenir l'agrément afin d'utiliser toute technologie de cryptage. Les propriétaires de systèmes n'utilisent pas de technologies de cryptage dans les systèmes de production sans autorisation préalable.

4. Le propriétaire du système consulte le LISO du département pour les questions relatives à la sécurité des SIC.

5. Le propriétaire du système réexamine au moins une fois par an les mesures de sécurité appliquées à un système, y compris son plan de sécurité.

6. Lorsqu'un incident de sécurité survient dans un SIC par lequel il est indiqué que le SIC ne peut plus protéger de manière adéquate les ICUE, le propriétaire du système en informe le LSO et contacte immédiatement l'autorité d'homologation de sécurité pour obtenir des conseils sur la marche à suivre. Dans ce cas, l'homologation peut être suspendue et le système peut être mis hors service jusqu'à ce que des mesures correctives appropriées aient été prises.

7. Le propriétaire du système apporte à tout moment à l'autorité d'homologation de sécurité un soutien total dans ses tâches relatives à l'homologation du SIC.

Article 10

Autorité opérationnelle chargée de l'assurance de l'information

L'autorité opérationnelle chargée de l'assurance de l'information pour chaque SIC:

a) établit la documentation relative à la sécurité conformément aux politiques et lignes directrices en matière de sécurité, en particulier le plan de sécurité, les SecOP se rapportant au système et la documentation cryptographique dans le cadre du processus d'homologation du SIC;

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

c) participe à la sélection des mesures et dispositifs de sécurité TEMPEST, si le plan de sécurité l'exige, et, en coopération avec l'autorité TEMPEST, veille à ce qu'ils soient installés et entretenus en toute sécurité;

d) contrôle la mise en œuvre et l'application des SecOP se rapportant au fonctionnement du système;

e) gère et traite les produits cryptographiques, en collaboration avec l'autorité de distribution cryptographique, afin d'assurer la bonne conservation du matériel cryptographique et des biens contrôlés et, si nécessaire, d'assurer la génération de variables cryptographiques;

f) procède à des analyses, révisions et tests en matière de sécurité, en particulier pour produire les rapports de risque pertinents, conformément aux exigences de l'autorité d'homologation de sécurité;

g) dispense une formation en matière d'assurance de l'information propre à chaque SIC;

h) mette en œuvre et gère des mesures de sécurité propres à chaque SIC.

CHAPITRE 4

Responsable local de sécurité

Article 11

Désignation du LSO

1. Le LSO et les LSO adjoints sont des fonctionnaires ou des agents temporaires.

2. Tous les LSO et LSO adjoints sont titulaires d'une autorisation de sécurité valable permettant d'accéder aux ICUE jusqu'au niveau SECRET UE/EU SECRET et au niveau TRÈS SECRET UE/EU TOP SECRET si nécessaire. Le LSO ou le LSO adjoint obtient l'autorisation de sécurité avant sa désignation.

3. Les représentations de la Commission peuvent demander à l'autorité de sécurité de la Commission d'accorder une dérogation aux exigences énoncées aux paragraphes 1 et 2.

Article 12

Procédures d'exploitation de sécurité (SecOP) pour les zones sécurisées

1. Le LSO du département de la Commission concerné établit des SecOP pour chaque zone sécurisée relevant de sa responsabilité.

2. Le LSO veille à ce que les SecOP portent notamment sur les exigences suivantes:

a) seuls les membres du personnel titulaires d'une autorisation de sécurité en cours de validité et ayant un besoin avéré d'accéder à des documents classifiés CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont autorisés à accéder sans escorte à une zone sécurisée pendant les heures de bureau;

b) l'accès sans escorte à une zone sécurisée en dehors des heures de bureau n'est accordé qu'au LSO du département, au(x) RCO de la zone sécurisée, à leurs adjoints et au personnel autorisé de la direction Sécurité de la direction générale Ressources humaines et sécurité;

c) les dispositifs d'enregistrement et de communication tels que les téléphones portables, les ordinateurs, les caméras ou d'autres dispositifs intelligents ne sont pas admis à l'intérieur des zones sécurisées sans l'autorisation préalable de l'autorité de sécurité de la Commission; toute dérogation est demandée à l'avance à l'autorité de sécurité de la Commission; le LSO fait office de point de contact;

d) l'ensemble du personnel interne ou externe qui a besoin d'accéder à une zone sécurisée mais ne remplit pas les critères énoncés au point a) ci-dessus est escorté et supervisé à tout moment par un membre du personnel dûment autorisé; tout accès de ce type à une zone sécurisée est consigné dans un journal de bord tenu à l'entrée de la zone sécurisée;

e) le LSO veille à ce que les systèmes de détection des intrusions qui surveillent une zone sécurisée soient actifs et fonctionnent correctement à tout moment, et gère tous les mots de passe, clés, codes d'identification personnels ou autres mécanismes d'accès et d'authentification s'y rapportant;

f) les alarmes dans une zone sécurisée sont signalées à la direction Sécurité de la direction générale Ressources humaines et sécurité, qui en informe immédiatement le LSO;

g) le LSO du département dans lequel la zone sécurisée est située tient un registre de chaque intervention à la suite d'une alarme ou d'un incident de sécurité;

h) des procédures doivent être mises en place pour faire face à une alarme ou à une autre situation d'urgence à l'intérieur de la zone sécurisée, y compris s'agissant de l'évacuation du personnel et de la nécessité d'assurer une réaction rapide d'une équipe d'urgence placée sous l'autorité de l'autorité de sécurité de la Commission et des services d'urgence externes si nécessaire;

i) le LSO signale immédiatement à l'autorité de sécurité de la Commission tout manquement à la sécurité survenant à l'intérieur d'une zone sécurisée ou impliquant une zone sécurisée afin de déterminer la réponse appropriée;

j) les bureaux, locaux et coffres-forts individuels situés à l'intérieur d'une zone sécurisée doivent être fermés à clé lorsqu'ils sont laissés sans surveillance;

k) le personnel évite de discuter d'informations classifiées dans les couloirs ou d'autres zones communes de la zone sécurisée lorsque des personnes non autorisées se trouvent à proximité.

Article 13

Clés et combinaisons de sécurité

1. Le LSO a la responsabilité générale d'assurer le traitement et le stockage appropriés des clés et combinaisons utilisées dans les zones sécurisées ou d'y accéder. Les clés et combinaisons sont stockées dans un meuble de sécurité et sont protégées au moins au même niveau que le matériel auquel elles donnent accès.

2. Le LSO tient un registre des meubles de sécurité et chambres fortes, ainsi qu'une liste à jour de tous les membres du personnel qui y ont accès sans escorte.

3. Le LSO tient un registre des clés des meubles de sécurité et chambres fortes, faisant notamment mention des membres du personnel auxquels lesdites clés sont assignées. Un reçu est conservé pour chaque clé remise, indiquant notamment l'identification de la clé, son destinataire ainsi que la date et l'heure.

4. Les clés et combinaisons ne sont remises qu'aux membres du personnel qui ont besoin d'en connaître et qui ont obtenu l'autorisation appropriée d'accéder aux ICUE. Le LSO récupère toute clé lorsque ces conditions ne sont plus remplies.

5. Le LSO conserve les clés de rechange et une trace écrite de chaque combinaison dans des enveloppes individuelles scellées, opaques, signées et datées, à fournir par le membre du personnel chargé des clés. Ces enveloppes sont conservées dans un meuble de sécurité prévu pour le niveau de classification le plus élevé du matériel stocké dans le meuble ou la chambre forte concernés.

6. Si, lors d'un changement de combinaison ou de clé, une enveloppe présente des signes d'altération ou de détérioration, le LSO traite cet incident comme un incident de sécurité et en informe immédiatement l'autorité de sécurité de la Commission.

7. Les modifications des combinaisons des meubles de sécurité dans les zones sécurisées sont effectuées sous la supervision du LSO. Les combinaisons sont réinitialisées au moins tous les 12 mois et dans les cas suivants:

a) à la réception d'un nouveau meuble ou à l'installation d'une nouvelle serrure (en particulier, les combinaisons par défaut doivent être modifiées immédiatement);

b) en cas de compromission, réelle ou présumée;

c) lorsque l'accès d'une personne possédant une combinaison n'est plus nécessaire.

8. Le LSO conserve une trace des dates des modifications des combinaisons visées au paragraphe 7.

Article 14

Plans d'évacuation et de destruction d'urgence des ICUE

1. Le LSO aide le chef de département à établir des plans d'évacuation et de destruction d'urgence des ICUE, sur la base des orientations fournies par la HR.DS.

2. Le LSO veille à ce que tout équipement nécessaire au fonctionnement des plans prévus au paragraphe 1 soit facilement disponible et maintenu en bon état de fonctionnement.

3. Le LSO, conjointement avec les fonctionnaires désignés dans les plans prévus au paragraphe 1, réexamine l'état de préparation des plans au moins tous les 12 mois et prend toutes les mesures nécessaires pour les mettre à jour.

Article 15

Autorisations de sécurité

1. Le LSO tient un registre de tous les postes au sein du département qui nécessitent une autorisation de sécurité de la Commission et du personnel occupant ces postes. L'exigence d'une autorisation de sécurité doit être précisée dans l'avis de vacance au cours de la procédure de recrutement et notifiée au candidat lors de l'entretien.

2. Le LSO supervise toutes les demandes d'autorisation de sécurité pour l'accès aux ICUE. Le LSO est le point de contact au sein du département et assure la liaison avec l'autorité de sécurité de la Commission pour les autorisations de sécurité.

3. Le LSO introduit la demande d'engagement de la procédure d'autorisation de sécurité à l'égard du membre du personnel concerné et veille à ce que ledit membre du personnel retourne rapidement le questionnaire d'habilitation de sécurité nationale à l'autorité de sécurité de la Commission.

4. Le LSO veille à ce que les membres du personnel disposant d'une habilitation de sécurité dans le département suivent la séance d'information obligatoire sur les ICUE afin d'obtenir leur autorisation de sécurité.

5. Le LSO se concerte régulièrement avec le service des ressources humaines du département pour obtenir des informations sur tout changement concernant des postes nécessitant une autorisation de sécurité et informe immédiatement l'autorité de sécurité de la Commission de tout changement de ce type.

6. Le LSO informe l'autorité de sécurité de la Commission de l'arrivée d'un nouveau membre du personnel détenteur d'une habilitation de sécurité existante pour occuper un poste exigeant de son titulaire qu'il dispose d'une autorisation de sécurité.

7. Le LSO veille à ce que les membres du personnel du département suivent l'intégralité de la procédure de renouvellement de l'habilitation de sécurité dans les délais requis. Tout membre du personnel qui refuse de suivre l'intégralité de la procédure est transféré à un poste pour lequel il n'est pas nécessaire de disposer d'une autorisation de sécurité.

Article 16

Bureau d'ordre pour les ICUE

1. Lorsqu'un département gère un bureau d'ordre pour les ICUE, le LSO supervise les activités des RCO en ce qui concerne le traitement des ICUE et le respect des règles de sécurité relatives à la protection des ICUE.

2. Le LSO effectue les contrôles suivants au moins tous les 12 mois et en cas de changement d'un RCO ou d'un RCO adjoint:

a) une vérification d'un échantillon de documents du bureau d'ordre pour les ICUE pour confirmer leur statut et l'exactitude du registre des documents classifiés;

b) une vérification d'un échantillon de reçus et de fiches de transmission pour la diffusion d'ICUE au bureau d'ordre pour les ICUE et au départ de celui-ci;

c) un contrôle d'un échantillon de certificats de destruction.

3. Au moins une fois par mois, le LSO effectue des contrôles par sondage portant sur le registre des documents classifiés et sur les documents classifiés reçus récemment afin de s'assurer que les documents sont correctement enregistrés.

4. Toutes les vérifications sont consignées dans le registre des documents classifiés.

Article 17

Autres responsabilités en matière de sécurité

Les autres responsabilités du LSO en matière de sécurité sont définies dans une note de sécurité portant notamment sur la sécurité physique des personnes, locaux et autres biens, ainsi que sur les informations.

CHAPITRE 5

Agent contrôleur (RCO)

Article 18

Désignation du RCO

1. Le RCO et les RCO adjoints sont des fonctionnaires ou des agents temporaires.

2. Tous les RCO et RCO adjoints sont titulaires d'une autorisation de sécurité valable permettant d'accéder aux ICUE jusqu'au niveau SECRET UE/EU SECRET et au niveau TRÈS SECRET UE/EU TOP SECRET si nécessaire. Le RCO ou le RCO adjoint obtient l'autorisation de sécurité avant sa désignation.

3. Les représentations de la Commission peuvent demander à l'autorité de sécurité de la Commission d'accorder une dérogation aux exigences énoncées aux paragraphes 1 et 2.

Article 19

Responsabilités

1. Les RCO enregistrent les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur à des fins de sécurité:

a) lorsqu'elles arrivent dans un département de la Commission ou le quittent; ou

b) lorsqu'elles arrivent dans un SIC ou le quittent.

2. Les RCO enregistrent tous les événements survenus au cours du cycle de vie de toutes les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur. Les RCO veillent également à la tenue d'un registre de toutes les informations classifiées RESTREINT UE/EU RESTRICTED ou de leur équivalent qui sont échangées avec des pays tiers et des organisations internationales. Cela se fait en coordination avec le bureau d'ordre pour les ICUE géré par le secrétariat général.

3. Le RCO enregistre les documents classifiés CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur dans le registre des documents classifiés et veille à ce qu'ils soient conservés en toute sécurité dans le bureau d'ordre pour les ICUE.

4. Le RCO assiste le personnel de la Commission dans la création et l'envoi d'informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur.

5. Lorsque des documents classifiés CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont reçus d'autres départements ou de parties externes, le RCO veille à ce que l'accusé de réception soit dûment renvoyé à l'expéditeur.

6. Avant de permettre à un membre du personnel d'accéder à un document classifié détenu par le bureau d'ordre pour les ICUE, le RCO vérifie auprès du LSO que le membre du personnel dispose d'une autorisation de sécurité accordée par l'autorité de sécurité de la Commission.

7. Le RCO enregistre tous les membres du personnel non autorisés à avoir accès au bureau d'ordre pour les ICUE sans escorte qui y entrent et en sortent, et il les accompagne pendant toute la durée de leur visite.

8. Lorsqu'un membre du personnel emporte un document pour consultation en dehors du bureau d'ordre pour les ICUE, le RCO veille à ce que ledit membre du personnel ait connaissance des mesures de sécurité compensatoires appropriées et à ce que le membre du personnel rapporte le document dès qu'il n'en a plus besoin. Le RCO rappelle au personnel de rapporter ce document dans les meilleurs délais.

9. Le bureau d'ordre pour les ICUE délivre un certificat de courrier si les documents classifiés sont transportés en main propre en dehors du pays où se trouve le bureau d'ordre.

10. Les instructions détaillées à l'intention des RCO concernant l'enregistrement des documents classifiés sont consignées dans une note de sécurité.

Article 20

Déclassement et déclassification

Le RCO assiste les départements auteurs dans le processus de réexamen des ICUE enregistrées afin de déterminer si le niveau de classification initial est toujours approprié ou si le document peut être déclassé ou déclassifié.

Article 21

Destruction

1. Les RCO sont responsables de la destruction des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et d'un niveau de classification supérieur par des moyens approuvés, le cas échéant en présence de témoins disposant d'une habilitation de sécurité.

2. Les RCO enregistrent toute destruction d'informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et d'un niveau de classification supérieur dans le registre des documents classifiés et conservent les certificats de destruction correspondants dans le bureau d'ordre pour les ICUE.

Article 22

Tâches supplémentaires

1. Le RCO fournit toute l'assistance nécessaire au LSO lorsque celui-ci exerce des activités de surveillance dans le bureau d'ordre pour les ICUE.

2. Le RCO signale tout incident de sécurité présumé ou réel au LSO, qui les signale à son tour à l'autorité de sécurité de la Commission.

3. Le RCO du bureau d'ordre pour les ICUE d'un département de la Commission organisant une réunion classifiée au niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur prépare les ICUE qui seront traitées au cours de la réunion et assure la coordination avec l'organisateur de la réunion afin de veiller à ce que tous les documents et reçus soient traités conformément aux règles applicables.

CHAPITRE 6

Dispositions finales

Article 23

Transparence

La présente décision est portée à la connaissance du personnel de la Commission et de toutes les personnes auxquelles elle s'applique, et est publiée au *Journal officiel de l'Union européenne*.

Article 24

La présente décision entre en vigueur le jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Fait à Bruxelles, le 7 avril 2022.

Par la Commission,
au nom de la présidente,
Gertrud INGESTAD
Directrice générale
Direction générale des ressources humaines et de la sécurité