DÉCISIONS

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

LA COMMISSION EUROPÉENNE,

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

vu le traité instituant la Communauté européenne de l'énergie atomique,

considérant ce qui suit:

(1) Les systèmes d'information et de communication de la Commission font partie intégrante de son fonctionnement. Les incidents de sécurité informatique peuvent dès lors avoir des conséquences graves sur ses activités ainsi que sur les tiers, y compris les particuliers, les entreprises et les États membres.

(2) Il existe de nombreuses menaces susceptibles de porter atteinte à la confidentialité, à l'intégrité ou à la disponibilité des systèmes d'information et de communication de la Commission et des informations qui y sont traitées. Il peut notamment s'agir d'accidents, d'erreurs, d'attaques délibérées et de phénomènes naturels, qui doivent être reconnus comme des risques opérationnels.

(3) Les systèmes d'information et de communication (SIC) doivent être fournis avec un niveau de protection proportionné à la probabilité, aux effets et à la nature des risques auxquels ils sont exposés.

(4) L'objectif de la sécurité informatique à la Commission devrait être de faire en sorte que les SIC de la Commission protègent les informations qu'ils traitent et fonctionnent comme ils le doivent, quand ils le doivent, sous le contrôle d'utilisateurs légitimes.

(5) La politique de sécurité informatique de la Commission devrait être mise en œuvre d'une manière qui soit cohérente avec les politiques sur la sécurité au sein de la Commission.

(6) La direction de la sécurité de la direction générale des ressources humaines et de la sécurité a la responsabilité générale de la sécurité au sein de la Commission, sous l'autorité et la responsabilité du membre de la Commission chargé des questions de sécurité.

(7) L'approche de la Commission devrait tenir compte des initiatives politiques de l'Union européenne et de la législation en matière de sécurité des réseaux et de l'information, des normes du secteur et des bonnes pratiques, afin de se conformer à l'ensemble de la législation applicable et de permettre l'interopérabilité et la compatibilité.

(8) Des mesures appropriées devraient être élaborées et appliquées par les services de la Commission chargés des systèmes d'information et de communication; les mesures de sécurité informatique pour la protection des systèmes d'information et de communication devraient faire l'objet d'une coordination au sein de la Commission pour assurer leur efficacité et leur efficience.

(9) Les règles et procédures concernant l'accès à l'information dans le contexte de la sécurité informatique, y compris la gestion des incidents relevant de la sécurité informatique, devraient être proportionnées à la menace pour la Commission ou son personnel et conformes aux principes énoncés dans le règlement (CE) n° 45/2001 du Parlement européen et du Conseil [1] relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes de l'Union et à la libre circulation de ces données, et tenir compte du principe du secret professionnel, tel que prévu à l'article 339 du TFUE.

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

(10) Les politiques et règles applicables aux systèmes d'information et de communication traitant des informations classifiées de l'Union européenne (ICUE), des informations sensibles non classifiées et des informations non classifiées doivent être en parfaite conformité avec les décisions de la Commission (UE, Euratom) 2015/443 ([1]) et (UE, Euratom) 2015/444 ([2]).

(11) La Commission doit réviser et mettre à jour les dispositions relatives à la sécurité des systèmes d'information et de communication qu'elle utilise.

(12) Il convient dès lors d'abroger la décision C(2006) 3602 de la Commission,

A ADOPTÉ LA PRÉSENTE DÉCISION:

CHAPITRE 1

DISPOSITIONS GÉNÉRALES

Article premier

Objet et champ d'application

1. La présente décision s'applique à tous les systèmes d'information et de communication (SIC) détenus, acquis, gérés ou exploités par ou pour le compte de la Commission et à toute utilisation desdits SIC par la Commission.

2. La présente décision définit les objectifs, les principes de base, l'organisation et les responsabilités en ce qui concerne la sécurité de ces SIC, en particulier pour les services de la Commission qui détiennent, acquièrent, gèrent ou exploitent des SIC, y compris ceux fournis par un prestataire de services informatiques interne. Lorsqu'un SIC est fourni, détenu, géré ou exploité par un tiers en vertu d'une convention bilatérale ou d'un contrat avec la Commission, les termes de la convention ou du contrat sont conformes à la présente décision.

3. La présente décision s'applique à tous les services de la Commission et à toutes les agences exécutives. Lorsqu'un SIC de la Commission est utilisé par d'autres organismes ou institutions en vertu d'une convention bilatérale avec la Commission, les termes de la convention sont conformes à la présente décision.

4. Nonobstant toute indication spécifique concernant des groupes particuliers de personnel, la présente décision s'applique aux membres de la Commission, au personnel de la Commission relevant du statut des fonctionnaires de l'Union européenne (ci-après le «statut») ainsi que du régime applicable aux autres agents de l'Union (ci-après le «RAA») ([3]), aux experts nationaux détachés auprès de la Commission (ci-après les «END») ([4]), aux prestataires de services externes et à leur personnel, aux stagiaires et à toute personne ayant accès aux SIC relevant du champ d'application de la présente décision.

5. La présente décision s'applique à l'Office européen de lutte antifraude (OLAF), dans la mesure où cela est compatible avec la législation de l'Union et la décision 1999/352/CE, CECA, Euratom de la Commission ([5]). En particulier, les mesures prévues dans la présente décision, y compris les consignes, les inspections, les enquêtes et les mesures équivalentes, ne peuvent s'appliquer au SIC de l'OLAF si elles ne sont pas compatibles avec l'indépendance de la fonction d'enquête de l'OLAF et/ou avec la confidentialité des informations obtenues par l'OLAF dans l'exercice de cette fonction.

Article 2

Définitions

Aux fins de la présente décision, les définitions suivantes s'appliquent:

1) «responsable»: qui doit répondre d'actes, décisions et performances;

([1]) Décision (UE, Euratom) 2015/443 de la Commission du 13 mars 2015 relative à la sécurité au sein de la Commission (JO L 72 du 17.3.2015, p. 41).

([2]) 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 (JO L 72 du 17.3.2015, p. 53).

([3]) Établi par le règlement (CEE, Euratom, CECA) nº 259/68 du Conseil du 29 février 1968 fixant le statut des fonctionnaires des Communautés européennes ainsi que le régime applicable aux autres agents de ces Communautés, et instituant des mesures particulières temporairement applicables aux fonctionnaires de la Commission (statut des fonctionnaires) (JO L 56 du 4.3.1968, p. 1).

([4]) Décision de la Commission du 12 novembre 2008 relative au régime applicable aux experts nationaux détachés et aux experts nationaux en formation professionnelle auprès des services de la Commission [C(2008) 6866 final].

([5]) Décision 1999/352/CE, CECA, Euratom de la Commission du 28 avril 1999 instituant l'Office européen de lutte antifraude (OLAF) (JO L 136 du 31.5.1999, p. 20).

2) «CERT-UE»: équipe d'intervention en cas d'urgence informatique pour les institutions et agences de l'Union européenne. Elle a pour mission d'aider les institutions européennes à se protéger contre les attaques intentionnelles et malveillantes qui compromettraient l'intégrité de leurs biens informatiques et nuiraient aux intérêts de l'Union. Le domaine d'activité de la CERT-UE couvre la prévention, la détection, l'intervention et la récupération;

3) «service de la Commission»: tout service ou direction générale de la Commission ou tout cabinet d'un membre de la Commission;

4) «autorité de sécurité de la Commission»: rôle prévu dans la décision (UE, Euratom) 2015/444;

5) «système d'information et de communication» ou «SIC»: tout système permettant le traitement d'informations sous forme électronique, avec l'ensemble des moyens nécessaires pour le faire fonctionner, y compris l'infrastructure, l'organisation, le personnel et les ressources d'information. Cette définition recouvre les applications professionnelles, les systèmes informatiques partagés, les services externalisés et dispositifs installés chez les utilisateurs finaux.

6) «conseil d'administration» (CMB): la plus haute instance de contrôle sur la gestion des questions opérationnelles et administratives au sein de la Commission;

7) «propriétaire des données»: personne chargée de garantir la protection et l'utilisation d'un ensemble de données spécifique géré par un SIC;

8) «ensemble de données»: ensemble d'informations qui sert à un processus donné ou à une activité spécifique de la Commission;

9) «procédure de secours»: ensemble prédéfini de méthodes et de responsabilités permettant de réagir aux situations d'urgence afin d'éviter des répercussions majeures sur la Commission;

10) «politique de sécurité de l'information»: ensemble d'objectifs en matière de sécurité de l'information, qui sont ou doivent être définis, mis en œuvre et contrôlés. Il s'agit, de manière non limitative, des décisions (UE, Euratom) 2015/444 et (UE, Euratom) 2015/443;

11) «comité de pilotage de la sécurité informatique» (CPSI): organe de gouvernance qui soutient le CMB dans ses tâches liées à la sécurité informatique;

12) «prestataire de services informatiques interne»: service de la Commission fournissant des services informatiques partagés;

13) «sécurité informatique» ou «sécurité des SIC»: préservation de la confidentialité, de l'intégrité et de la disponibilité des SIC et des ensembles de données qu'ils traitent;

14) «orientations en matière de sécurité informatique»: mesures recommandées mais non obligatoires aidant à respecter les normes de sécurité informatique ou servant de référence lorsque aucune norme n'est applicable;

15) «incident de sécurité informatique»: événement qui pourrait porter atteinte à la confidentialité, l'intégrité ou la disponibilité d'un SIC;

16) «mesure de sécurité informatique»: mesure technique ou organisationnelle visant à atténuer les risques de sécurité informatique;

17) «besoin de sécurité informatique»: définition précise et non ambiguë des niveaux de confidentialité, d'intégrité et de disponibilité associés à une information ou un système informatique afin de définir le niveau de protection requis;

18) «objectif de sécurité informatique»: déclaration d'intention pour contrer des menaces spécifiques et/ou répondre à des exigences ou des hypothèses organisationnelles spécifiques liées à la sécurité;

19) «plan de sécurité informatique»: documentation sur les mesures de sécurité informatique nécessaires pour satisfaire les besoins de sécurité informatique d'un SIC;

20) «politique de sécurité informatique»: ensemble d'objectifs en matière de sécurité informatique, qui sont ou doivent être définis, mis en œuvre et contrôlés. Elle se compose de la présente décision et de ses règles d'application;

21) «exigence de sécurité informatique»: besoin de sécurité informatique formalisé par un processus prédéfini;

22) «risque de sécurité informatique»: effet qu'une menace pour la sécurité informatique pourrait avoir sur un SIC en exploitant une vulnérabilité. En tant que tel, un risque de sécurité informatique est caractérisé par deux facteurs: 1) l'incertitude, c'est-à-dire la probabilité qu'une menace pour la sécurité informatique cause un événement indésirable, et 2) l'incidence, c'est-à-dire les conséquences qu'un tel événement indésirable pourrait avoir pour un SIC;

23) «normes de sécurité informatique»: mesures de sécurité informatique obligatoires spécifiques qui facilitent la mise en œuvre et le soutien à la politique de sécurité informatique;

24) «stratégie de sécurité informatique»: ensemble de projets et d'activités qui sont conçus pour atteindre les objectifs de la Commission et qui doivent être définis, mis en œuvre et contrôlés;

25) «menace pour la sécurité informatique»: facteur qui pourrait conduire à un événement indésirable susceptible de porter atteinte à un SIC. Ces menaces peuvent être accidentelles ou délibérées et se caractérisent par des éléments menaçants, des cibles potentielles et des méthodes d'attaque;

26) «responsable local de la sécurité informatique» (*Local Informatics Security Officer* — LISO): agent de liaison responsable de la sécurité informatique d'un service de la Commission;

27) «données à caractère personnel», «traitement de données à caractère personnel», «responsable du traitement» et «fichier de données à caractère personnel» ont la même signification que dans le règlement (CE) n° 45/2001, et notamment son article 2;

28) «traitement des informations»: toutes les fonctions d'un SIC relatives aux ensembles de données, y compris la création, la modification, l'affichage, le stockage, la transmission, la suppression et l'archivage des informations. Le traitement des informations peut être fourni par le SIC comme un ensemble de fonctionnalités aux utilisateurs et comme services informatiques à d'autres SIC;

29) «secret professionnel»: protection des données commerciales qui, par leur nature, sont couvertes par le secret professionnel, et notamment les renseignements relatifs aux entreprises et concernant leurs relations commerciales ou les éléments de leur prix de revient, conformément à l'article 339 du TFUE;

30) «garant»: ayant l'obligation d'agir et de prendre des décisions pour atteindre les résultats souhaités;

31) «sécurité au sein de la Commission»: sécurité des personnes, des biens et des informations au sein de la Commission, en particulier l'intégrité physique des personnes et des biens, l'intégrité, la confidentialité et la disponibilité des informations et des systèmes d'information et de communication, ainsi que le fonctionnement sans entrave des activités de la Commission;

32) «service informatique partagé»: service fourni par un SIC à d'autres SIC pour le traitement de l'information;

33) «propriétaire du système»: personne chargée de l'ensemble des procédures d'acquisition, de développement, d'intégration, de modification, d'exploitation, de maintenance et de démantèlement d'un SIC;

34) «utilisateur»: toute personne qui utilise les fonctionnalités fournies par un SIC, que ce soit à l'intérieur ou à l'extérieur de la Commission.

Article 3

Principes de sécurité informatique au sein de la Commission

1. La sécurité informatique au sein de la Commission est fondée sur les principes de légalité, de transparence, de proportionnalité et de responsabilité.

2. Les aspects liés à la sécurité informatique sont pris en compte dès le début de l'élaboration et de la mise en œuvre des SIC de la Commission. La direction générale de l'informatique et la direction générale des ressources humaines et de la sécurité participent à cette démarche dans leurs domaines de compétence respectifs.

3. Une sécurité informatique efficace garantit que les caractéristiques suivantes atteignent des niveaux appropriés:

a) authenticité: garantie que l'information est véridique et émane de sources dignes de foi;

b) disponibilité: fait d'être accessible et utilisable, à la demande d'une entité autorisée;

c) confidentialité: propriété selon laquelle les informations ne sont pas divulguées à des personnes ou à des entités non autorisées et l'accès à ces informations n'est pas accordé à des processus non autorisés;

d) intégrité: propriété consistant à préserver l'exactitude et le caractère complet des informations et éléments;

e) non-répudiation possibilité de prouver qu'une action ou un événement a eu lieu, de sorte qu'il ne peut être contesté par la suite;

f) protection des données à caractère personnel: la fourniture de garanties appropriées en matière de données à caractère personnel dans le plein respect du règlement (CE) nº 45/2001;

g) secret professionnel: protection des données commerciales qui, par leur nature, sont couvertes par le secret professionnel, et notamment les renseignements relatifs aux entreprises et concernant leurs relations commerciales ou les éléments de leur prix de revient, conformément à l'article 339 du TFUE.

4. La sécurité informatique est fondée sur un processus de gestion des risques. Ce processus a pour but de déterminer les niveaux de risque en matière de sécurité informatique et de définir les mesures de sécurité permettant de ramener ces risques à un niveau adéquat, pour un coût proportionné.

5. Tous les SIC sont recensés, attribués à un propriétaire de système et consignés dans un inventaire.

6. Les exigences de sécurité de l'ensemble des SIC sont déterminées en fonction des besoins de sécurité de ces derniers et des besoins de sécurité des informations qu'ils traitent. Les SIC qui fournissent des services à d'autres SIC peuvent être conçus pour soutenir des niveaux donnés de besoins en matière de sécurité.

7. Les plans et les mesures de sécurité informatique doivent être proportionnés aux besoins de sécurité des SIC.

Les processus liés à ces principes et activités sont décrits plus en détail dans les modalités d'application.

CHAPITRE 2

ORGANISATION ET RESPONSABILITÉS

Article 4

Conseil d'administration (CMB)

Le CMB prend la responsabilité globale de la gouvernance de la sécurité informatique dans son ensemble au sein de la Commission.

Article 5

Comité de pilotage de la sécurité informatique (CPSI)

1. Le CPSI est présidé par le secrétaire général adjoint chargé de la gouvernance de la sécurité informatique à la Commission. Ses membres représentent les aspects commerciaux et intérêts relevant de la technologie et de la sécurité dans tous les services de la Commission et sont issus de la direction générale de l'informatique, la direction générale des ressources humaines et de la sécurité, de la direction générale du budget et, suivant une rotation tous les deux ans, de quatre autres directions de la Commission concernées car la sécurité informatique constitue une préoccupation importante pour leurs activités. Ces membres sont issus de l'encadrement supérieur.

2. Le CPSI soutient le CMB dans ses tâches liées à la sécurité informatique. Il assume la responsabilité globale de la gouvernance de la sécurité informatique dans son ensemble au sein de la Commission.

3. Le CPSI recommande la politique de sécurité informatique de la Commission en vue de son adoption par cette dernière.

4. Le CPSI examine et fait rapport deux fois par an au CMB sur les questions liées à la gouvernance ainsi que sur les questions liées à la sécurité informatique, y compris les graves incidents de sécurité informatique.

5. Le CPSI surveille et évalue la mise en œuvre globale de la présente décision et fait rapport au CMB.

6. Sur la proposition de la direction générale de l'informatique, le CPSI examine, approuve et surveille la mise en œuvre de la stratégie glissante en matière de sécurité informatique. Il fait rapport à ce sujet au CMB.

7. Le CPSI surveille, évalue et contrôle le paysage des risques informatiques et est habilité à émettre des demandes formelles d'amélioration chaque fois que cela est nécessaire.

Les processus liés à ces responsabilités et activités sont décrits plus en détail dans les règles d'application.

Article 6

Direction générale des ressources humaines et de la sécurité

En ce qui concerne la sécurité informatique, la direction générale des ressources humaines et de la sécurité assume les responsabilités suivantes. Elle:

1) assure la cohérence entre la politique de sécurité informatique et la politique de sécurité de l'information de la Commission;

2) établit un cadre pour l'autorisation de l'utilisation des technologies de chiffrement pour le stockage et la communication d'informations par les SIC;

3) informe la direction générale de l'informatique des menaces spécifiques qui pourraient avoir un impact significatif sur la sécurité des SIC et des ensembles de données qu'ils traitent;

4) effectue des inspections dans le domaine de la sécurité informatique afin d'évaluer la conformité des SIC de la Commission avec la politique de sécurité et communique les résultats au CPSI.

5) établit un cadre pour l'autorisation d'accès aux SIC de la Commission à partir de réseaux externes et pour les règles de sécurité connexes appropriées et élabore les normes et lignes directrices correspondantes en matière de sécurité informatique, en étroite collaboration avec la direction générale de l'informatique;

6) propose des principes et règles pour la sous-traitance des SIC afin de maintenir un contrôle approprié de la sécurité de l'information;

7) élabore les normes de sécurité informatique et les lignes directrices correspondantes en ce qui concerne l'article 6, en étroite collaboration avec la direction générale de l'informatique.

Les processus liés à ces responsabilités et activités sont décrits plus en détail dans les règles d'application.

Article 7

Direction générale de l'informatique

En ce qui concerne la sécurité informatique globale de la Commission, la direction générale de l'informatique assume les responsabilités suivantes. Elle:

1) élabore des normes et des lignes directrices en matière de sécurité informatique, sauf dans les cas prévus à l'article 6, en coopération étroite avec la direction générale des ressources humaines et de la sécurité, afin d'assurer la cohérence entre la politique de sécurité informatique et la politique de sécurité de l'information de la Commission et les soumet au CPSI;

2) évalue les méthodes de gestion des risques en matière de sécurité informatique, les processus et les résultats de l'ensemble des services de la Commission et en rend compte régulièrement au CPSI;

3) propose une stratégie glissante de sécurité informatique pour révision et approbation par le CPSI et adoption ultérieure par le CMB, et propose un programme comprenant notamment la planification des projets et des activités de mise en œuvre de la stratégie de sécurité informatique;

4) contrôle l'exécution de la stratégie de sécurité informatique de la Commission et en rend compte régulièrement au CPSI;

5) contrôle les risques de sécurité informatique et les mesures de sécurité mises en œuvre dans les SIC de la Commission et en rend compte régulièrement au CPSI;

6) fait régulièrement rapport au CPSI sur la mise en œuvre globale et le respect de la présente décision;

7) après consultation de la direction générale des ressources humaines et de la sécurité, demande aux propriétaires des systèmes de prendre des mesures de sécurité spécifiques afin d'atténuer les risques de sécurité informatique pour les SIC de la Commission;

8) s'assure qu'il existe un catalogue adéquat de services de la direction générale de l'informatique de la sécurité informatique accessible aux propriétaires de systèmes et de données pour leur permettre d'assumer leurs responsabilités en matière de sécurité informatique et de se conformer à la politique et aux normes de sécurité informatique;

9) fournit une documentation appropriée aux propriétaires de systèmes et de données et consulte ceux-ci, le cas échéant, sur les mesures de sécurité informatique mises en œuvre pour leurs services informatiques afin de faciliter la conformité avec la politique de sécurité informatique et d'aider les propriétaires de systèmes à gérer les risques informatiques;

10) organise des réunions régulières du réseau des LISO et soutient ces derniers dans l'exercice de leurs fonctions;

11) définit les besoins de formation et coordonne les programmes de formation sur la sécurité informatique en coopération avec les services de la Commission, et élabore, met en œuvre et coordonne des campagnes de sensibilisation sur la sécurité informatique en étroite collaboration avec la direction générale chargée des ressources humaines;

12) s'assure que les propriétaires de systèmes, les propriétaires de données et les autres responsables de la sécurité informatique au sein des services de la Commission sont informés de la politique de sécurité informatique;

13) informe la direction générale des ressources humaines et de la sécurité de certains incidents et menaces pour la sécurité informatique et des exceptions à la politique de la Commission en matière de sécurité informatique qui ont été signalés par les propriétaires de systèmes et qui pourraient avoir une incidence significative sur la sécurité au sein de la Commission;

14) en ce qui concerne son rôle en tant que prestataire de services informatiques interne, fournit à la Commission un catalogue des services informatiques partagés procurant des niveaux de sécurité définis. Elle s'acquitte de cette tâche en évaluant, gérant et surveillant systématiquement les risques de sécurité informatique pour mettre en œuvre les mesures de sécurité permettant d'atteindre le niveau de sécurité défini.

Les processus connexes et les responsabilités plus détaillées sont précisés dans les règles d'application.

Article 8

Services de la Commission

En ce qui concerne la sécurité informatique au sein de son service, chaque chef de service de la Commission:

1) désigne officiellement, pour chaque SIC, un fonctionnaire ou un agent temporaire en qualité de propriétaire de système, qui sera responsable de la sécurité informatique du SIC en question, et désigne officiellement, pour chaque ensemble de données traité dans un SIC, un propriétaire des données qui doit appartenir à la même entité administrative que celle responsable du traitement des données pour les ensembles de données couverts par le règlement (CE) nº 45/2001;

2) désigne officiellement un responsable local de la sécurité informatique (LISO) qui puisse exercer ses responsabilités indépendamment des propriétaires de système et de données. Un LISO peut être désigné pour un ou plusieurs services de la Commission;

3) veille à ce que des évaluations des risques dans le domaine de la sécurité informatique et des plans de sécurité informatique appropriés aient été mis en œuvre;

4) veille à ce qu'un résumé des risques et mesures de sécurité informatique soit communiqué régulièrement à la direction générale de l'informatique;

5) veille, avec le soutien de la direction générale de l'informatique, à ce que les processus, procédures et solutions appropriés soient en place pour assurer une détection, un signalement et une résolution efficaces des incidents de sécurité informatique relatifs à ses SIC;

6) lance une procédure d'urgence en cas de situations d'urgence en matière de sécurité informatique;

7) assume la responsabilité ultime de la sécurité informatique, notamment les responsabilités du propriétaire du système et du propriétaire des données;

8) détient les risques liés à ses SIC et ensembles de données;

9) résout les désaccords éventuels entre les propriétaires de systèmes et les propriétaires de données et, en cas de persistance du désaccord, porte l'affaire devant le CPSI en vue de sa résolution;

10) veille à ce que des plans et des mesures de sécurité informatique soient mis en œuvre et que les risques soient couverts de manière adéquate.

Les processus liés à ces responsabilités et activités sont décrits plus en détail dans les modalités d'application.

Article 9

Propriétaires de systèmes

1. Le propriétaire du système est responsable de la sécurité informatique du SIC, et est placé sous l'autorité du chef de service de la Commission.

2. En ce qui concerne la sécurité informatique, le propriétaire du système:

a) veille à la conformité du SIC avec la politique de sécurité informatique;

b) veille à ce que le SIC soit correctement enregistré dans l'inventaire ad hoc;

c) évalue les risques de sécurité informatique et détermine les besoins de sécurité informatique pour chaque SIC, en collaboration avec les propriétaires de données et en consultation avec la direction générale de l'informatique;

d) prépare un plan de sécurité, y compris, le cas échéant, le détail des risques évalués et toute mesure de sécurité supplémentaire requise;

e) met en œuvre les mesures de sécurité informatique appropriées et proportionnées aux risques mis en évidence, et suit les recommandations avalisées par le CPSI;

f) détecte toute dépendance vis-à-vis d'autres SIC ou services informatiques partagés et met en œuvre, si nécessaire, des mesures de sécurité fondées sur les niveaux de sécurité proposés par ces SIC ou services informatiques partagés;

g) gère et surveille les risques de sécurité informatique;

h) fait régulièrement rapport au chef du service de la Commission sur le profil de risque de son SIC en matière de sécurité informatique et rend compte à la direction générale de l'informatique des risques associés, des activités de gestion des risques et des mesures de sécurité prises;

i) consulte le LISO du ou des services compétents de la Commission sur les aspects de sécurité informatique;

j) publie des instructions pour les utilisateurs du SIC et des données connexes ainsi que sur les responsabilités des utilisateurs en rapport avec le SIC;

k) sollicite l'autorisation de la direction générale des ressources humaines et de la sécurité, en qualité d'autorité Crypto, pour tout SIC qui utilise des technologies de chiffrement;

l) consulte l'autorité de sécurité de la Commission au préalable concernant tout système traitant des informations classifiées de l'Union européenne;

m) veille à ce que les sauvegardes de toutes les clés de déchiffrement soient stockées dans un compte séquestre. La récupération des données chiffrées est effectuée seulement lorsqu'elle est autorisée conformément au cadre défini par la direction générale des ressources humaines et de la sécurité;

n) respecte les instructions données par le ou les responsables du traitement des données concernés quant à la protection des données à caractère personnel et à l'application des règles de protection des données à la sécurité du traitement;

o) signale à la direction générale de l'informatique toute exception à la politique de sécurité informatique de la Commission, y compris les motifs invoqués;

p) signale au chef du service de la Commission tout différend impossible à régler entre le propriétaire des données et le propriétaire du système, communique les incidents de sécurité informatique aux parties concernées en temps utile, le cas échéant, en fonction de leur gravité, comme prévu à l'article 15;

q) veille, pour les systèmes externalisés, à ce que les dispositions de sécurité informatique appropriées soient incluses dans les contrats d'externalisation et que les incidents de sécurité survenant dans les SIC externalisés soient signalés conformément à l'article 15;

r) veille à ce que les SIC fournissant des services informatiques partagés atteignent un niveau de sécurité défini et clairement documenté, et que des mesures de sécurité soient mises en œuvre pour que lesdits SIC parviennent au niveau de sécurité défini.

3. Les propriétaires de systèmes peuvent déléguer officiellement une partie ou la totalité de leurs tâches en matière de sécurité informatique, mais ils demeurent responsables de la sécurité informatique de leurs SIC.

Les processus liés à ces responsabilités et activités sont décrits plus en détail dans les modalités d'application.

Article 10

Propriétaires de données

1. Le propriétaire des données est garant de la sécurité informatique d'un ensemble de données spécifique auprès du chef du service de la Commission et est responsable de la confidentialité, de l'intégrité et de la disponibilité de l'ensemble de données.

2. En ce qui concerne cet ensemble de données, le propriétaire des données:

a) veille à ce que tous les ensembles de données sous sa responsabilité soient correctement classés conformément aux décisions (UE, Euratom) 2015/443 et (UE, Euratom) 2015/444;

b) définit les besoins en matière de sécurité de l'information et en informe les propriétaires de systèmes;

c) participe à l'évaluation des risques pesant sur le SIC;

d) signale au chef du service de la Commission tout différend impossible à régler entre le propriétaire des données et le propriétaire du système;

e) communique les incidents de sécurité informatique, comme prévu à l'article 15.

3. Les propriétaires de données peuvent déléguer officiellement une partie ou la totalité de leurs tâches en matière de sécurité informatique, mais ils conservent leurs responsabilités telles que définies au présent article.

Les processus liés à ces responsabilités et activités sont décrits plus en détail dans les modalités d'application.

Article 11

Responsables locaux de la sécurité informatique (LISO)

En ce qui concerne la sécurité informatique, le LISO:

a) identifie proactivement les propriétaires de systèmes, les propriétaires de données et les autres responsables de la sécurité informatique au sein des services de la Commission et les informe de la politique de sécurité informatique;

b) se concerte avec la direction générale de l'informatique, dans le cadre du réseau LISO, sur les questions liées à la sécurité informatique dans les services de la Commission;

c) assiste aux réunions régulières des LISO;

d) garde une vue d'ensemble du processus de gestion des risques de sécurité de l'information ainsi que de l'élaboration et de la mise en œuvre des plans de sécurité du système d'information;

e) conseille les propriétaires de données, les propriétaires de systèmes et les chefs des services de la Commission sur les questions liées à la sécurité informatique;

f) coopère avec la direction générale de l'informatique pour la diffusion des bonnes pratiques en matière de sécurité informatique et propose des programmes spécifiques de sensibilisation et de formation;

g) fait rapport sur la sécurité informatique, sur les lacunes recensées et sur les améliorations possibles aux chefs de services de la Commission.

Les processus liés à ces responsabilités et activités sont décrits plus en détail dans les règles d'application.

Article 12

Utilisateurs

1. En ce qui concerne la sécurité informatique, les utilisateurs:

a) se conforment à la politique de sécurité informatique et aux instructions émises par le propriétaire du système concernant l'utilisation de chaque SIC;

b) communiquent les incidents de sécurité informatique, comme prévu à l'article 15.

2. L'utilisation du SIC de la Commission en violation de la politique de sécurité informatique ou des instructions édictées par le propriétaire du système peut donner lieu à des procédures disciplinaires.

Les processus liés à ces responsabilités et activités sont décrits plus en détail dans les modalités d'application.

CHAPITRE 3

EXIGENCES ET OBLIGATIONS EN MATIÈRE DE SÉCURITÉ

Article 13

Mise en œuvre de la présente décision

1. L'adoption des règles d'application mentionnées à l'article 6, ainsi que des normes et lignes directrices connexes, fera l'objet d'une décision d'habilitation de la Commission en faveur du membre de la Commission chargé des questions de sécurité.

2. L'adoption de toutes les autres règles d'application liées à la présente décision, ainsi que des normes et lignes directrices connexes en matière de sécurité informatique, fera l'objet d'une décision d'habilitation de la Commission en faveur du membre de la Commission chargé de l'informatique.

3. Le CPSI approuve les règles d'application, les normes et les lignes directrices visées aux paragraphes 1 et 2 ci-dessus, préalablement à leur adoption.

Article 14

Caractère contraignant

1. Le respect des dispositions exposées dans la politique et les normes de sécurité informatique est obligatoire.

2. Le non-respect de la politique et des normes de sécurité informatique est passible d'une sanction disciplinaire conformément aux traités, au statut et au RAA, de sanctions contractuelles et/ou de poursuites judiciaires en vertu du droit national.

3. La direction générale de l'informatique est informée de toute exception à la politique de sécurité informatique.

4. Dans l'hypothèse où le CPSI estime qu'il existe un risque inacceptable persistant pour un SIC de la Commission, la direction générale de l'informatique soumet, en coopération avec le propriétaire du système, des mesures d'atténuation au CPSI pour approbation. Ces mesures peuvent consister, entre autres, en un renforcement des contrôles et des rapports, et en des restrictions, voire une interruption, de service.

5. Le CPSI impose, le cas échéant, la mise en œuvre des mesures d'atténuation approuvées. Il peut aussi recommander au directeur général de la direction générale des ressources humaines et de la sécurité d'ouvrir une enquête administrative. La direction générale de l'informatique fait rapport au CPSI sur toute situation où des mesures d'atténuation sont imposées.

Les processus liés à ces responsabilités et activités sont décrits plus en détail dans les règles d'application.

Article 15

Gestion des incidents de sécurité informatique

1. La direction générale de l'informatique est responsable de la fourniture de la principale capacité de réaction opérationnelle aux incidents de sécurité informatique au sein de la Commission européenne.

2. La direction générale des ressources humaines et de la sécurité, en sa qualité de partie prenante contribuant à la réaction aux incidents de sécurité informatique:

a) a le droit d'accéder à des informations succinctes pour tous les incidents et à un rapport complet sur demande;

b) participe aux groupes de gestion de crise des incidents de sécurité informatique et aux procédures d'urgence en matière de sécurité informatique;

c) est chargée des relations avec les services répressifs et de renseignement;

d) effectue l'analyse criminalistique concernant la cybersécurité conformément à l'article 11 de la décision (UE, Euratom) 2015/443;

e) décide s'il y a lieu de lancer une enquête formelle;

f) informe la direction générale de l'informatique de tous les incidents de sécurité informatique susceptibles de présenter un risque pour d'autres SIC.

3. Des communications régulières ont lieu entre la direction générale de l'informatique et la direction générale des ressources humaines et de la sécurité afin d'échanger des informations et de coordonner la gestion des incidents de sécurité, en particulier les incidents liés à la sécurité informatique qui pourraient nécessiter une enquête formelle.

4. Les services de coordination en cas d'incident de l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union européenne (CERT-UE) peuvent être utilisés à l'appui du processus de gestion des incidents le cas échéant, ainsi que pour le partage des connaissances avec les autres institutions et agences de l'Union européenne susceptibles d'être affectées.

5. Les propriétaires de systèmes d'information impliqués dans un incident lié à la sécurité informatique:

a) informent immédiatement leur chef de service de la Commission, la direction générale de l'informatique, la direction générale des ressources humaines, le LISO et, le cas échéant, le propriétaire des données, de tout incident majeur de sécurité informatique, en particulier s'il implique une violation de la confidentialité des données;

b) coopèrent et suivent les instructions données par les autorités concernées de la Commission en matière de communication, de réaction et de remise en état.

6. Les utilisateurs signalent en temps utile tous les incidents de sécurité informatique, réels ou présumés, au helpdesk informatique compétent.

7. Les propriétaires de données signalent en temps utile tous les incidents de sécurité informatique, réels ou présumés, à l'équipe de réaction aux incidents de sécurité informatique compétente.

8. La direction générale de l'informatique, avec l'aide des autres parties prenantes, est chargée de traiter tout incident de sécurité informatique affectant des SIC de la Commission qui ne sont pas externalisés.

9. La direction générale de l'informatique informe les services de la Commission concernés des incidents de sécurité informatique, ainsi que les LISO concernés et, le cas échéant, la CERT-EU en fonction du besoin d'en connaître.

10. La direction générale de l'informatique fait régulièrement rapport au CPSI sur les principaux incidents de sécurité informatique affectant les SIC de la Commission.

11. Le LISO concerné doit, sur demande, avoir accès aux archives de l'incident de sécurité concernant le SIC du service de la Commission.

12. En cas d'incident majeur lié à la sécurité informatique, la direction générale de l'informatique est le point de contact pour la gestion des situations de crise en ce qu'elle coordonne les groupes de gestion de crise des incidents de sécurité informatique.

13. En cas d'urgence, le directeur général de la direction générale de l'informatique peut décider de lancer une procédure d'urgence en matière de sécurité informatique. La direction générale de l'informatique met en place des procédures d'urgence à approuver par le CPSI.

14. La direction générale de l'informatique fait rapport sur l'exécution des procédures d'urgence au CPSI et aux chefs des services de la Commission concernés.

Les processus liés à ces responsabilités et activités sont décrits plus en détail dans les règles d'application.

CHAPITRE 4

DISPOSITIONS FINALES

Article 16

Transparence

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

Article 17

Rapport avec d'autres actes

Les dispositions de la présente décision sont sans préjudice de la décision (UE, Euratom) 2015/443, de la décision (UE, Euratom) 2015/444, du règlement (CE) n° 45/2001, du règlement (CE) n° 1049/2001 du Parlement européen et du Conseil ([1]), de la décision 2002/47/CE, CECA, Euratom de la Commission ([2]), du règlement (UE, Euratom) n° 883/2013 du Parlement européen et du Conseil ([3]) et de la décision 1999/352/CE, CECA, Euratom.

Article 18

Abrogation et mesures transitoires

La décision C(2006) 3602 du 16 août 2006 est abrogée.

Les règles d'application et les normes de sécurité informatique adoptées en vertu de l'article 10 de la décision C(2006) 3602 restent en vigueur, pour autant qu'elles ne soient pas en contradiction avec la présente décision, jusqu'à ce qu'elles soient remplacées par les règles d'application et les normes à adopter en vertu de l'article 13 de la présente décision. Toute référence à l'article 10 de la décision C(2006) 3602 s'entend comme une référence à l'article 13 de la présente décision.

Article 19

Entrée en vigueur

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

Fait à Bruxelles, le 10 janvier 2017.

Par la Commission
Le président
Jean-Claude JUNCKER

([1]) 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 (JO L 145 du 31.5.2001, p. 43).
([2]) Décision 2002/47/CE, CECA, Euratom de la Commission du 23 janvier 2002 modifiant son règlement intérieur (JO L 21 du 24.1.2002, p. 23).
([3]) Règlement (UE, Euratom) n° 883/2013 du Parlement européen et du Conseil du 11 septembre 2013 relatif aux enquêtes effectuées par l'Office européen de lutte antifraude (OLAF) et abrogeant le règlement (CE) n° 1073/1999 du Parlement européen et du Conseil et le règlement (Euratom) n° 1074/1999 du Conseil (JO L 248 du 18.9.2013, p. 1).