JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 423 du 29 mai 2018

Arrêté grand-ducal du 9 mai 2018 portant fixation de la gouvernance en matière de gestion de la sécurité de l'information.

Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau,

Vu l'article 76 de la Constitution ;

Vu l'arrêté royal grand-ducal du 9 juillet 1857 portant organisation du Gouvernement grand-ducal, tel qu'il a été modifié ;

Vu l'arrêté grand-ducal du 28 janvier 2015 portant constitution des Ministères ;

Sur le rapport de Notre Premier Ministre, Ministre d'État et après délibération du Gouvernement en Conseil ;

Arrêtons :

Art. 1er.

Aux fins du présent arrêté grand-ducal, on entend par :

- « Sécurité de l'information » : sécurité autour des systèmes d'information classifiés et non classifiés installés et exploités par l'État,
- « Systèmes de communication et d'information » : tout système d'information et de communication et tout autre système électronique traitant des informations,
- « Système de communication et d'information classifié » : tout système de communication et d'information où sont traitées des pièces classifiées telles que définies dans la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité,
- « Informations classifiées » : toute information ou tout matériel identifié comme tel par la classification de sécurité de l'entité correspondante, dont la divulgation non autorisée pourrait porter atteinte à des degrés divers aux intérêts de l'entité correspondante,
- « Bureau d'ordre central » : entité nationale responsable d'organiser la réception, la comptabilisation, la distribution et la destruction des pièces classifiées,
- « Bureau d'ordre auxiliaire » : entité décentralisée d'un département ministériel, administration, service ou autre structure spécifique responsable de la réception, de la comptabilisation, de la distribution et de la destruction des pièces classifiées de ce département ministériel, administration, service ou autre structure,
- « Agence nationale de la sécurité des systèmes d'information (ANSSI) » : autorité nationale en matière de sécurité des systèmes d'information classifiés et non classifiés installés et exploités par l'État.

Art. 2.

La gouvernance de la gestion de la sécurité de l'information classifiée et non classifiée, est organisée autour des trois autorités suivantes :

- autorité régulatrice
- autorité opérationnelle
- autorité homologative.

Art. 3.

(1) Le Haut-Commissariat à la Protection Nationale assure la fonction d'ANSSI. Celle-ci est considérée comme autorité régulatrice.

(2) L'ANSSI a pour missions :

1. de définir, après concertation des acteurs concernés, la politique générale de sécurité de l'information non classifiée ;
2. de définir, en étroite collaboration avec l'autorité homologative et opérationnelle, une politique de sécurité et des lignes directrices en matière de l'information classifiée ;
3. de définir, à la demande des acteurs ayant dans leurs attributions les domaines spécifiques et en étroite concertation avec ces derniers, les politiques et lignes directrices de sécurité de l'information pour les domaines spécifiques ;
4. d'émettre, à la demande des acteurs concernés, des recommandations d'implémentation des politiques et lignes directrices de sécurité de l'information ;
5. d'assister, à leur demande, les entités dans l'implémentation des politiques et lignes directrices de sécurité de l'information ;
6. de définir, en concertation avec les acteurs concernés, une approche de gestion des risques, en vue de constituer un plan d'évaluation et d'identification des risques et d'accompagner, à la demande, les entités dans l'analyse et la gestion des risques ;
7. de définir, en concertation avec les acteurs concernés des indicateurs de suivi de l'implémentation des politiques et lignes directrices de sécurité de l'information et de rédiger périodiquement un rapport de synthèse permettant d'assurer un pilotage haut niveau ;
8. d'assister le Haut-Commissariat à la Protection nationale dans sa tâche d'élaboration de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information (« stratégie cybersécurité ») d'une part et dans sa mission de protection des infrastructures critiques pour ce qui est du volet de la sécurité de l'information de celles-ci d'autre part ;
9. de conseiller l'Institut national d'administration publique, respectivement, à leur demande, les entités dans la définition d'un programme de formation dans le domaine de la sécurité de l'information ;
10. de promouvoir la sécurité de l'information, notamment par le biais de mesures de sensibilisation à l'adresse des dirigeants et des utilisateurs ;
11. d'assurer la fonction d'autorité Tempest.

Dans sa fonction d'autorité Tempest, il lui incombe :

a) de veiller à la conformité des systèmes de communication et d'information classifiés aux stratégies et lignes directrices TEMPEST ;
b) d'approuver les contre-mesures TEMPEST pour les installations et les produits destinés à protéger des informations classifiées jusqu'à un certain niveau de classification dans leur environnement opérationnel.

Art. 4.

Sont considérées comme autorités opérationnelles, les administrations et services ayant dans leurs attributions les missions telles que définies d'une part par la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État ainsi que d'autre part par le présent texte. Les missions sont les suivantes :

1. concevoir, développer, déployer, exploiter et maintenir des systèmes de communication et d'information classifiés nationaux et internationaux ;
2. acquérir les produits essentiels à la protection des systèmes de communication et d'information classifiés ;
3. assurer la formation des utilisateurs des systèmes de communication et d'information classifiés ;
4. assurer le respect des règles et procédures de sécurité, notamment en cas d'interconnexion de systèmes ;
5. assurer la fonction d'Autorité de distribution cryptographique ;
6. assumer la fonction d'autorité responsable du fonctionnement d'un bureau d'ordre central et de la supervision des bureaux d'ordre auxiliaires.

En tant qu'autorité de distribution cryptographique, il leur incombe :

a) de gérer et d'assurer la manutention, le stockage et la distribution du matériel cryptographique en toute sécurité ;

b) d'assurer le transfert et la reprise du matériel cryptographique auprès des personnes ou des services utilisateurs.

Art. 5.

La fonction d'autorité d'agrément cryptographique indépendante est exercée sous l'autorité du Centre des Technologies de l'Information de l'État.

Art. 6.

Est considérée comme autorité homologative l'Autorité nationale de Sécurité, qui a pour missions celles définies par la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité.

Art. 7.

Les principes et les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne s'appliquent mutatis mutandis à chaque fois qu'aucune disposition n'existe au niveau national pour la sécurité des informations classifiées nationales.

Art. 8.

L'arrêté grand-ducal du 10 février 2015 1. portant fixation de la gouvernance en matière de gestion de la sécurité de l'information 2. modifiant l'arrêté grand-ducal du 30 juillet 2013 déterminant l'organisation et les attributions du Centre gouvernemental de traitement des urgences informatiques, aussi dénommé « Computer Emergency Response Team Gouvernemental » est abrogé.

Art. 9.

Notre Premier Ministre, Ministre d'État, est chargé de l'exécution du présent arrêté qui sera publié au Journal officiel du Grand-Duché de Luxembourg.

Le Premier Ministre,
Ministre d'État,
Xavier Bettel

Château de Berg, le 9 mai 2018.
Henri