

PROJET DE REGLEMENT ILR/N22/X DU DD-MM-YYYY

**PORTANT SUR LA NOTIFICATION DES MESURES DE SÉCURITÉ À PRENDRE PAR LES OPÉRATEURS
FOURNISSANT DES SERVICES ESSENTIELS.**

NISS

La Direction de l'Institut Luxembourgeois de Régulation (ci-après l'« Institut »),

Vu la loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant 1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale (ci-après la « Loi »), notamment son article 8, paragraphes 1 à 3 ;

Vu le règlement ILR/N19/1 du 5 novembre 2019 portant sur la fixation des services essentiels – Service NISS (ci-après le « règlement ILR/N19/1 ») ;

Vu la consultation publique relative au projet de règlement portant sur la notification des mesures de sécurité à prendre par les opérateurs de services essentiels du 13 juillet 2022 au 31 août 2022 ;

Arrête :

Art. 1^{er}. (1) Le présent règlement détermine la notification par les opérateurs de services essentiels des mesures visées à l'article 8 (1) et (2) de la Loi.

(2) La notification de ces mesures se fait par :

- a) une description des mesures en place comme détaillée à l'article 2 du présent règlement ;
- b) une analyse de risques liée au(x) service(s) essentiel(s) fourni(s) comme détaillée à l'article 3 du présent règlement ; et

- c) une liste des dépendances envers d'autres services essentiels comme détaillée à l'article 4 du présent règlement.

Art. 2. (1) La description visée à l'article 1^{er} (2) (a) du présent règlement comprend une liste de différentes mesures dans les domaines suivants :

- gouvernance et gestion des risques ;
- sécurité des ressources humaines ;
- sécurité des systèmes et des ressources ;
- gestion des opérations ;
- gestion des incidents ;
- gestion de la continuité de l'activité
- surveillance, inspection et test ; et
- sensibilisation aux menaces.

(2) Le détail et la portée des mesures à prendre en compte pour la description visée à l'article 1^{er} (2) (a) du présent règlement, sont à trouver dans le document « Formulaire Mesures » publié sur le site Internet de l'Institut, accessible via <https://www.serima.lu/mesures> et régulièrement mis à jour par l'Institut.

Art. 3. (1) L'analyse de risques liée au(x) service(s) essentiel(s) fourni(s) comprend au moins les informations suivantes :

- une liste des services essentiels fournis au Luxembourg ;
- les actifs primaires et secondaires nécessaires pour fournir ces services pris en compte ;
- les échelles de cotation des menaces, de l'impact et des vulnérabilités ;
- les critères d'acceptation des risques ;
- la liste des menaces prises en compte ;
- la liste des vulnérabilités appliquées pour chaque actif ;
- les impacts de chaque risque identifié ;
- les mesures mises en place pour minimiser les risques ;
- le choix de traitement des risques et le calendrier d'implémentation y relatif ; et
- l'évaluation des risques résiduels.

(2) L'Institut fournit des listes sectorielles contenant des actifs primaires et secondaires à considérer.

Art. 4. (1) L'opérateur de services essentiels fournit une liste des dépendances envers d'autres services essentiels.

(2) Au sens du présent règlement, une dépendance envers d'autres services essentiels est donnée pour un opérateur de service essentiel dans le cas où la fourniture de son/ses

propre(s) service(s) essentiel(s) nécessite(nt) le recours à un ou plusieurs autre(s) service(s) essentiel(s).

Art. 5. (1) La notification des mesures au sens des articles 2 à 4, se fait par le biais de :

- la plateforme SERIMA mise à disposition par l'Institut à travers la page web <https://www.serima.lu>; ou
- tout autre moyen jugé équivalent par l'Institut.

(2) La notification des mesures est à fournir dans un format exploitable par l'Institut ou dans un des formats indiqués par l'Institut sur sa page web à cette fin, accessible via <https://www.serima.lu/mesures>.

Art. 6. (1) L'Institut peut à tout moment demander aux opérateurs de services essentiels des informations nécessaires pour évaluer la sécurité de leurs réseaux et systèmes d'information, y compris les documents relatifs à leurs politiques de sécurité.

(2) Les opérateurs de services essentiels fournissent ces informations additionnelles en respectant les délais et le niveau de détail exigés par l'Institut dans sa demande.

Art. 7. La notification des mesures au sens des articles 2 à 4 du présent règlement est à soumettre annuellement et à chaque fois qu'un changement de la situation rend de nouvelles mesures nécessaires pour assurer un niveau de sécurité adapté et/ou approprié aux risques existants, conformément à l'article 5 du présent règlement, au plus tard pour les échéances suivantes :

<u>Secteur</u>	<u>Échéance</u>
- pour le secteur « Energie » au sens du règlement ILR/N19/1	15 octobre
- pour le secteur « Transports » au sens du règlement ILR/N19/1	15 novembre
- pour le secteur « Santé » au sens du règlement ILR/N19/1	15 février
- pour le secteur « Fourniture et distribution d'eau potable » au sens du règlement ILR/N19/1	15 mars
- pour le secteur « Infrastructures numériques » au sens du règlement ILR/N19/1	15 décembre

Art. 8. Le présent règlement sera publié au Journal officiel du Grand-Duché de Luxembourg et sur le site Internet de l'Institut.

**Pour l'Institut Luxembourgeois de Régulation
La Direction**

**Michèle Bram
Directrice adjointe**

**Camille Hierzig
Directeur adjoint**

**Luc Tapella
Directeur**