INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

PROJET DE REGLEMENT ILR/N26/X DU DD-MM-YYYY

PORTANT SUR LA NOTIFICATION DES MESURES DE SECURITE PRISES PAR LES ENTITES ESSENTIELLES.

NISS

La Direction de l'Institut Luxembourgeois de Régulation,

Vu la loi du 5 mai 2026 concernant des mesures destinées à assurer un niveau élevé de cybersécurité, notamment son article 12, paragraphes 1 et 3, article 21, paragraphe 1 et article 22, paragraphe 2 ;

Vu la consultation publique nationale (CP/N26/X) relative au projet de règlement portant sur la notification des mesures de sécurité prises par les entités essentielles du XX XX 2026 au XX XX 2026 ;

Vu le résultat de la consultation publique nationale mentionnée ci-dessus ;

Arrête :

Art. 1er. (1) Le présent règlement détermine la notification par les entités essentielles des mesures visées à l'article 12, paragraphes (1) et (2) de la loi du 5 mai 2026 concernant des mesures destinées à assurer un niveau élevé de cybersécurité (ci-après la « Loi »).

(2) La notification de ces mesures à l'Institut Luxembourgeois de Régulation (ci-après « l'Institut ») se fait par :

a) une description des mesures en place, comme détaillée à l'article 2 du présent règlement ;
b) une analyse des principaux scénarios de risques cyber liés aux activités ou à la fourniture des services de l'entité, comme détaillée à l'article 3 du présent règlement ;
c) un plan d'action pluriannuel, comme détaillé à l'article 4 du présent règlement ; et
d) à la demande de l'Institut, toute information liée aux mesures visées à l'article 12, paragraphes (1) et (2) de la Loi.

(3) En plus de la notification des mesures au sens du paragraphe 2 du présent article, les entités essentielles recensées en tant qu'entités critiques au sens de l'article 2, point 1° de la loi du 5 mai 2026 sur la résilience des entités critiques notifient :

- une liste des dépendances envers des fournisseurs ou prestataires de services directs, comme détaillée à l'article 5 du présent règlement.

(4) Dans le cadre de la fixation de ses priorités de supervision au sens de l'article 21, paragraphe 1er de la Loi, l'Institut peut adapter ses méthodes de supervision pour certaines catégories d'entités essentielles selon une approche basée sur les risques. Les entités concernées en seront informées par l'Institut avec un délai raisonnable.

Art. 2. (1) La description des mesures en place comprend au moins une liste de différentes mesures dans les domaines suivants :

a) Engagement et responsabilité de l'organe de direction ;
b) Politique relative à la sécurité des réseaux et des systèmes d'information ;
c) Politiques de gestion des risques ;
d) Gestion des incidents ;
e) Continuité des activités et gestion des crises ;
f) Sécurité de la chaîne d'approvisionnement ;
g) Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information ;
h) Politiques et procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité ;
i) Pratiques de base en matière de cyberhygiène et formation à la sécurité de l'information ;
j) Cryptographie ;
k) Sécurité des ressources humaines ;
l) Contrôle d'accès ;
m) Gestion des actifs ; et
n) Sécurité environnementale et physique.

(2) Le détail et la portée des mesures à prendre en compte pour cette description, sont à trouver dans le document « Mesures », régulièrement mis à jour et publié sur le site Internet de l'Institut, accessible via https://www.serima.lu/mesures.

Art. 3. (1) L'analyse des principaux scénarios de risques cyber liés aux activités ou la fourniture des services de l'entité essentielle comprend, pour chacun des principaux scénarios de risques cyber au moins les informations suivantes :

a) L'analyse et l'évaluation du niveau d'impact ;
b) L'analyse et l'évaluation de la probabilité de survenance ;
c) Le traitement des risques ; et
d) Le niveau de risque résiduel.

(2) Une liste des principaux scénarios de risques cyber génériques à analyser et à notifier à l'Institut est publiée dans le document « Analyse des principaux scénarios de risques

cyber », régulièrement mis à jour et publié sur le site Internet de l'Institut, accessible via https://www.serima.lu/mesures.

L'Institut peut identifier et ajouter à la liste du paragraphe 1er du présent article, des scénarios de risques cyber additionnels et spécifiques à certains secteur ou types d'entité.

Art. 4. (1) L'entité essentielle fournit un plan pluriannuel d'actions en cours ou planifiés visant à élever le niveau de cybersécurité de l'entité et adressant des points constatés dans le cadre de la description des mesures en place, au sens de l'article 2 du présent règlement et l'analyse des principaux scénarios de risques cyber, au sens de l'article 3 du présent règlement.

(2) Le plan d'action pluriannuel comprend au moins les informations suivantes :

a) L'action concrète en cours ou planifiée ;
b) Le(s) scénario(s) de risque mitigé(s) ;
c) La ou les mesure(s) adressée(s) ;
d) La date cible d'implémentation de l'action ;
e) Le responsable désigné pour l'exécution de l'action en question ; et
f) La priorité attribuée à l'implémentation de l'action.

(2) Le détail du plan d'action pluriannuel est à trouver dans le document « Plan d'action pluriannuel », régulièrement mis à jour et publié sur le site Internet de l'Institut, accessible via https://www.serima.lu/mesures.

Art. 5. (1) L'entité critique au sens de l'article 2, point 1° de la loi du 5 mai 2026 sur la résilience des entités critiques fournit en plus des mesures au sens des articles 2 à 4 du présent règlement, une liste des dépendances envers des fournisseurs ou prestataires de services directs.

(2) Au sens du présent règlement, une dépendance envers des fournisseurs ou prestataires de services directs est donnée pour une entité essentielle dans le cas où son activité ou la fourniture de son/ses propre(s) service(s) nécessite(nt) le recours à une ou plusieurs autre(s) entités.

(3) Le détail de la liste des dépendances est à trouver dans le document « Formulaire dépendances », régulièrement mis à jour et publié sur le site Internet de l'Institut, accessible via https://www.serima.lu/mesures.

Art. 6. (1) La notification des mesures au sens des articles 2 à 5 du présent règlement est à effectuer annuellement au plus tard **pour le 15 mars de l'année en question** et à chaque fois qu'un changement de la situation rend de nouvelles mesures nécessaires pour assurer un niveau de sécurité adapté ou approprié aux risques existants.

(2) La notification annuelle visée au paragraphe précédent est à effectuer indépendamment de la survenance de changements des mesures depuis la dernière notification.

(3) Les informations visées par l'article 1er, paragraphe 2, d) sont à notifier dans le délai indiqué dans le cadre de la demande de l'Institut.

Art. 7. (1) La notification des mesures au sens des articles 2 à 5 du présent règlement, se fait par le biais de :

a) la plateforme SERIMA mise à disposition par l'Institut à travers la page web https://www.serima.lu; ou
b) tout autre moyen sécurisé jugé équivalent par l'Institut.

(2) Les notifications visées au paragraphe premier du présent article sont 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. 8. (1) L'Institut peut à tout moment, conformément à l'article 22, paragraphe 2, point 5° de la Loi, demander aux entités essentielles des informations nécessaires à l'évaluation des mesures de gestion des risques en matière de cybersécurité adoptées par l'entité concernée, notamment les politiques de cybersécurité consignées par écrit.

(2) L'institut peut à tout moment, conformément à l'article 22, paragraphe 2, point 6° de la Loi, demander d'avoir accès à des données, à des documents et à toutes informations nécessaires à l'accomplissement de ses tâches de supervision.

(3) Les entités essentielles fournissent ces informations en respectant les délais et le niveau de détail exigés par l'Institut dans sa demande.

Art. 9. Le présent règlement abroge le règlement ILR/N22/7 du 15 septembre 2022 portant sur la notification des mesures de sécurité à prendre par les opérateurs de services essentiels, ainsi que le règlement ILR/N22/8 du 26 septembre 2022 portant sur la notification des mesures de sécurité à prendre par les entreprises fournissant des réseaux de communications publics et/ou des services de communications électroniques au public.

Art. 10. 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

Claude Rischette	**Sandra Wietor**	**Luc Tapella**
Directeur adjoint	**Directrice adjointe**	**Directeur**