



INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

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

PORTANT SUR LES MODALITES DE NOTIFICATION ET LES CRITERES DES INCIDENTS AYANT UN IMPACT
IMPORTANT

NISS

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

Vu la loi du 5 mai 2026 concernant des mesures destinées à assurer un niveau élevé de cybersécurité, notamment son article 14 paragraphes (1) et (3) ;

Vu le règlement d'exécution (UE) 2024/2690 de la Commission du 17 octobre 2024 établissant des règles relatives à l'application de la directive (UE) 2022/2555 pour ce qui est des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité et précisant plus en détail les cas dans lesquels un incident est considéré comme important, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance (ci-après le « Règlement d'exécution (UE) 2024/2690 ») ;

Vu la consultation publique nationale (CP/N26/xx) relative au projet de règlement portant sur les modalités de notification et les critères des incidents ayant un impact important du xxx au xxx ; et

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

Arrête :

Art. 1^{er}. (1) Les entités essentielles et importantes notifient à l'Institut tous les incidents ayant un impact important sur leur fourniture des services suivant les critères et seuils définis au présent règlement et ses annexes.

(2) Les incidents sont à notifier à l'Institut par l'intermédiaire de la plateforme SERIMA accessible via <https://serima.lu/notification> ou bien par le biais du lien [---

Page 1 / 5](https://niss-</p></div><div data-bbox=)

notification.ilr.lu ou par un autre moyen automatisé à définir préalablement avec l'Institut. Pour toute action ultérieure liée au même incident, le même moyen de communication est à utiliser.

- Art. 2.** (1) Un incident est considéré comme ayant un impact important sur la fourniture des services si au moins l'une des situations suivantes s'est présentée :
- a) le service fourni par une entité est, ou a été, partiellement ou totalement inaccessible ou indisponible pendant plus d'une heure, ou pour plus de 5% des utilisateurs de ce service au Luxembourg ;
 - b) il y a eu un accès non autorisé effectif au réseau et aux systèmes d'information d'une entité concernée, qui est suspecté d'être malveillant et est susceptible de causer une perturbation opérationnelle grave ;
 - c) l'incident a entraîné ou est susceptible d'entraîner un impact sur l'authenticité, l'intégrité ou la confidentialité (i) des réseaux, (ii) des services, ou (iii) des données stockées, traitées, transmises ou transformées liées à la fourniture d'un service par l'entité concernée, à condition que cet impact sur l'authenticité, l'intégrité ou la confidentialité ait touché plus de 50 utilisateurs au Luxembourg ;
 - d) l'incident a causé ou est susceptible de provoquer l'exfiltration de secrets d'affaires de l'entité concernée, au sens de l'article 2, point 1° de la loi du 26 juin 2019 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites ;
 - e) l'incident a eu ou est susceptible d'avoir un impact transfrontalier ou international ;
 - f) l'accès physique à l'infrastructure servant à fournir un service par l'entité est compromis ;
 - g) l'incident a engendré ou est susceptible d'engendrer un risque pour la sécurité, la sûreté ou la santé publique ;
 - h) l'incident a causé ou est susceptible de causer des dommages considérables à la santé d'une personne physique ;
 - i) l'incident a causé ou est susceptible de causer le décès d'une personne physique ;
 - j) l'incident a causé ou est susceptible de causer une perte financière directe d'au moins 500 000 euros ou d'au moins 5% du chiffre d'affaires annuel total de l'entité, le montant le plus faible étant retenu ;
 - k) l'incident a causé ou est susceptible de causer un préjudice matériel ou moral à une personne morale d'au moins 50 000 euros ou à une personne physique d'au moins 10 000 euros ;
 - l) l'incident remplit les critères définis dans les annexes au présent règlement conformément au paragraphe 5 du présent article.
- (2) Les interruptions de service programmées et les conséquences prévues des opérations de maintenance programmées et effectuées par les entités concernées ou pour leur compte ne sont pas considérées comme des incidents importants.

- (3) La durée de l'incident est la période qui s'écoule entre la perturbation de la prestation du service en termes de disponibilité, d'authenticité, d'intégrité ou de confidentialité jusqu'au moment de son rétablissement.
- (4) Les incidents qui, pris isolément, ne sont pas considérés comme des incidents importants au sens du paragraphe 1^{er} du présent article ou des annexes au présent règlement sont considérés collectivement comme un incident important à notifier lorsqu'ils remplissent l'ensemble des critères suivants :
- a) ils se sont produits au moins deux fois en six mois ;
 - b) ils ont la même cause originelle apparente ;
 - c) ils répondent collectivement aux critères énoncés au paragraphe 1^{er}, point j) du présent article.
- (5) Des critères supplémentaires ou spécifiques par secteur, type d'entité ou groupes d'entités peuvent être définis par l'Institut en annexe au présent règlement.
- (6) Le présent article ne s'applique pas aux entités essentielles et importantes visées par le Règlement d'exécution (UE) 2024/2690.

Art. 3. (1) Tout incident détecté pouvant avoir un impact important sur la fourniture des services doit faire l'objet d'une notification préliminaire à l'Institut sans retard injustifié et en tout état de cause dans les 24 heures de sa détection et ceci selon les modalités décrites à l'article 1^{er}, paragraphe 2 du présent règlement. La notification préliminaire contient une estimation quant au nombre d'utilisateurs potentiellement concernés, à la durée prévisionnelle de l'incident, à la suspicion d'un acte illicite ou malveillant, aux services concernés ainsi qu'une indication quant à un potentiel impact à caractère transfrontalier.

(2) Sans retard injustifié et en tout état de cause dans les soixante-douze heures après avoir eu connaissance de l'incident important, l'entité concernée soumet une notification d'incident, qui, le cas échéant, met à jour les informations visées au paragraphe 1^{er} et fournit une évaluation initiale de l'incident important, y compris de sa gravité et de son impact, ainsi que des indicateurs de compromission, lorsqu'ils sont disponibles. La notification d'incident se fera suivant les modalités décrites à l'article 1^{er}, paragraphe 2 du présent règlement.

(3) Au plus tard un mois après la présentation de la notification d'incident visée au paragraphe 2 du présent article, le déclarant fait parvenir un rapport final à l'Institut comprenant au moins les informations suivantes :

- les informations de contact ;
- les services impactés ;
- les informations sur l'impact et la gravité de l'incident ;
- une description détaillée de l'incident ;
- la date de la première détection de l'incident ;
- la date du début de l'incident (si connue) ;
- l'impact transfrontalier de l'incident ;
- le type de menace ou la cause profonde de l'incident ;

- l'information si l'incident a eu un impact sur la disponibilité, l'intégrité, la confidentialité ou l'authenticité du réseau et des systèmes d'information de l'entité ; et
- à la demande de l'Institut, toute information relative à l'incident.

(4) Dans l'hypothèse où, après l'analyse interne de l'incident par le déclarant, il s'avère que l'incident, ayant déjà fait l'objet d'une notification conformément aux paragraphes 1^{er} ou 2 du présent article, ne répond finalement pas à au moins une des situations énumérées par l'article 2, paragraphe 1^{er} ou par les annexes du présent règlement, une notification n'est pas requise. Le déclarant partage ses conclusions et les informations y relatives sans délai à l'Institut selon les modalités décrites à l'article 1^{er}, paragraphe 2 du présent règlement.

(5) Par dérogation au paragraphe 2 du présent article, un prestataire de services de confiance notifie les incidents importants qui ont un impact sur la fourniture de ses services de confiance, sans retard injustifié et en tout état de cause dans les vingt-quatre heures après avoir eu connaissance de l'incident important.

(6) L'entité partage avec l'Institut toute information divulguée par elle aux médias qui a trait à un incident ayant eu un impact important sur la fourniture des services suivant les modalités décrites à l'article 1^{er}, paragraphe 2 du présent règlement. Dans le cas où un incident a fait l'objet d'une médiatisation indépendamment de la volonté de l'entité concernée, celle-ci informera l'Institut quant à la véracité des faits.

Art. 4. L'Institut peut à tout moment demander des informations additionnelles sur un incident conformément à l'article 22 (2) points 5°, 6° et 7°, respectivement l'article 23 (2), points 4°, 5° et 6° de la loi du 5 mai 2026 concernant des mesures destinées à assurer un niveau élevé de cybersécurité. Les entités fournissent ces informations additionnelles en respectant les délais et le niveau de détail exigés par l'Institut dans sa demande.

Art. 5. Le présent règlement abroge les règlements suivants :

- Règlement ILR/N19/1 du 5 novembre 2019 portant sur la fixation des services essentiels - Service NISS ;
- Règlement ILR/N21/1 du 9 juin 2021 portant définition des paramètres et modalités en relation avec la notification d'un incident ayant un impact significatif sur la fourniture d'un service numérique par les fournisseurs de services numériques à signaler à l'Institut – NISS ;
- Règlement ILR/N21/2 du 4 octobre 2021 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur eau potable – NISS ;
- Règlement ILR/N22/1 du 22 février 2022 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur transport - sous-secteur transport ferroviaire – NISS ;

- Règlement ILR/N22/2 du 15 juin 2022 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur transport - Sous-secteur transport routier – NISS ;
- Règlement ILR/N22/3 du 3 août 2022 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur de l'énergie - Sous-secteur gaz – NISS ;
- Règlement ILR/N22/4 du 3 août 2022 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur de l'énergie - Sous-secteur électricité – NISS ;
- Règlement ILR/N22/5 du 3 août 2022 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur santé – NISS ;
- Règlement ILR/N22/6 du 3 août 2022 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur infrastructure numérique – NISS ;
- Règlement ILR/N23/1 du 2 mai 2023 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur transport sous-secteur transport aérien – NISS ; et
- Règlement ILR/N23/3 du 20 juillet 2023 portant définition de critères et de seuils en relation avec l'impact significatif sur le fonctionnement des réseaux ou des services de communications électroniques – NISS.

Art. 7. 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
Directeur adjoint

Sandra Wietor
Directrice adjointe

Luc Tapella
Directeur