

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

**PORTANT DÉFINITION DES MODALITÉS DE NOTIFICATION ET DES CRITÈRES DES INCIDENTS AYANT UN
IMPACT SIGNIFICATIF SUR LA CONTINUITÉ DES SERVICES ESSENTIELS DU SECTEUR DES
INFRASTRUCTURES NUMÉRIQUES**

NISS

La Direction de l'Institut Luxembourgeois de Régulation,

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, notamment son article 8, paragraphe 4 et paragraphe 5 ;

Vu le règlement ILR/N19/1 du 5 novembre 2019 portant sur la fixation des services essentiels et notamment son article 1^{er}, paragraphe 4 ;

Vu les groupes de travail instaurés par l'Institut en septembre 2021 ;

Vu la consultation publique relative au projet de règlement portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur des infrastructures numériques du 10 janvier 2022 au 11 février 2022 ;

Arrête :

- Art. 1^{er}.** (1) Les opérateurs de services essentiels du secteur des infrastructures numériques notifient à l'Institut tous les incidents ayant un impact significatif sur la continuité des services essentiels.
- (2) Un incident est considéré comme ayant un impact significatif sur la continuité des services essentiels si au moins l'une des situations suivantes s'est présentée :

a) le service fourni par un opérateur de services essentiels est, ou a été, indisponible selon les critères suivants :

1° Pour l'activité d'interconnexion pour l'échange de trafic Internet :

- 50 pourcent des utilisateurs finaux sont impactés ;
- entre 30 et 50 pourcent des utilisateurs finaux sont impactés pendant au moins 30 minutes ;
- entre 10 et 30 pourcent des utilisateurs finaux sont impactés pendant au moins 4 heures ;
ou
- entre 1 et 10 pourcent des utilisateurs finaux sont impactés pendant au moins 8 heures ;

2° Pour l'activité de résolution de noms de domaine :

- indisponibilité du service *Domaine Name System* (DNS ou système de noms de domaine) (par exemple 25 pourcent des domaines non-résolus ou une diminution d'au moins 50 pourcent du trafic DNS ou indisponibilité des serveurs de nom) ;
- impact significatif sur le service DNS pendant au moins 30 minutes (par exemple entre 5 et 25 pourcent des domaines non-résolus ou diminution de 10 à 50 pourcent du trafic DNS ou indisponibilité de 3 serveurs de nom) ;
- impact moyen sur le service DNS pendant au moins 1 heure (par exemple entre 2 et 5 pourcent des domaines non-résolus ou diminution de 5 à 10 pourcent du trafic DNS ou indisponibilité de 2 serveurs de nom) ; ou
- impact faible sur le service DNS pendant au moins 6 heures (par exemple entre 1 et 2 pourcent des domaines non-résolus ou diminution de 1 à 5 pourcent du trafic DNS ou indisponibilité d'un serveur de nom) ;

3° Pour l'activité d'attribution des noms de domaine et la gestion du registre des noms de domaines de premier niveau :

- dégradation du service pendant au moins 1 heure ; ou
- service indisponible pendant au moins 1 minute ;

b) l'incident a entraîné une perte de disponibilité, d'authenticité, d'intégrité ou de confidentialité de données stockées, traitées, transmises ou transformées ou bien des services connexes offerts ou accessibles par l'intermédiaire d'un réseau et d'un système informatique de l'opérateur de services essentiels qui a touché plus de 50 utilisateurs finaux au Luxembourg ;

c) l'incident a engendré un risque pour la sécurité ou la sûreté publique ou a entraîné un décès ;

d) l'incident a causé un préjudice matériel d'au moins 50 000 EUR à un utilisateur.

(3) Le pourcentage des utilisateurs touchés est calculé pour chaque service essentiel par rapport au nombre total des personnes utilisant ce service du même opérateur.

(4) 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.

(5) Les incidents sont à notifier à l'Institut par l'intermédiaire de la plateforme <https://serima.lu/notification> ou bien par le biais du lien <https://niss-notification.ilr.lu> ou par moyen automatisé à définir préalablement ensemble avec l'Institut. Pour toute action ultérieure liée au même incident, le même moyen de communication est à favoriser.

Art. 2. (1) Tout incident détecté pouvant avoir un impact significatif sur la continuité des services essentiels ou dont la cause pourrait être en relation avec les réseaux ou systèmes d'information doit faire l'objet d'une pré-notification à l'Institut endéans les 24 heures de sa détection et ceci selon les modalités décrites à l'article 1, paragraphe 5 du présent règlement. La pré-notification contient une estimation quant au nombre d'utilisateurs potentiellement concernés, à la durée prévisionnelle de l'incident, aux services concernés ainsi qu'une indication quant à un potentiel impact à caractère transfrontalier.

(2) Lorsqu'après une analyse interne de l'incident par le déclarant il s'avère que cet incident répond aux critères énoncés à l'article 1, paragraphe 2 du présent règlement, le déclarant fait parvenir une notification complète à l'Institut endéans un délai de 15 jours après la détection de l'incident et ceci suivant les modalités décrites à l'article 1, paragraphe 5 du présent règlement.

Cette notification complète doit au moins comprendre les informations suivantes :

- les informations de contact ;
- les services essentiels impactés ;
- les informations sur l'impact de l'incident ;
- une description de l'incident ;
- la date de la première observation de l'incident ;
- la date du début de l'incident (si connue) ;
- l'impact géographique de l'incident ;
- la cause de l'incident ; et
- 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'opérateur de services essentiels.

(3) Dans le cas où des informations additionnelles sur l'incident deviendraient disponibles ultérieurement, l'opérateur de services essentiels procédera à une notification additionnelle après la notification complète. Cette notification additionnelle est à réaliser selon les modalités décrites à l'article 1, paragraphe 5 du présent règlement.

(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 pré-notification, ne répond finalement pas aux critères fixés par l'article 1, paragraphe 2 du présent règlement, une notification complète n'est pas requise. Le déclarant en informe de suite l'Institut selon les modalités décrites à l'article 1, paragraphe 5 du présent règlement.

(5) L'opérateur de services essentiels partage avec l'Institut toute information divulguée par lui aux médias qui a trait à un incident ayant eu un impact significatif sur la continuité des services essentiels.

- Art. 3.** L'Institut peut à tout moment demander des informations additionnelles sur un incident. 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. 4.** L'Institut signale aux autres États membres de l'Union européenne touchés si l'incident est susceptible d'avoir un impact significatif sur la continuité des services essentiels dans ces États membres, tout en préservant la sécurité et les intérêts commerciaux de l'opérateur de services essentiels ainsi que la confidentialité des informations communiquées dans sa notification.
- Art. 5.** Le présent règlement sera publié au Journal officiel du Grand-Duché de Luxembourg et sera également disponible 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