



Règlement grand-ducal du 21 février 2018 fixant la structure des plans de sécurité et de continuité de l'activité des infrastructures critiques.

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

Vu l'article 8 de la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale ;

Vu l'avis de la Chambre de commerce ;

L'avis de la Chambre des métiers ayant été demandé ;

Notre Conseil d'État entendu ;

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

Arrêtons :

Art. 1^{er}.

Le plan de sécurité et de continuité de l'activité comprend au moins les éléments suivants :

- 1° caractéristiques de l'infrastructure critique ;
- 2° identification, analyse et évaluation des risques ;
- 3° mesures de réduction des risques et stratégies préventives ;
- 4° dispositif de continuité de l'activité.

Le plan de sécurité et de continuité de l'activité couvre les éléments visés en annexe.

Art. 2.

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

*Le Premier Ministre,
Ministre d'État,
Xavier Bettel*

Palais de Luxembourg, le 21 février 2018.
Henri

Annexe – Plan de sécurité et de continuité de l'activité type

Chapitre 1^{er} - Caractéristiques de l'infrastructure critique

- 1° localisation de l'infrastructure (adresse, numéros de téléphone, plan d'accès) ;
- 2° nature des activités ;
- 3° organisation hiérarchique ;
- 4° données de contact du correspondant pour la sécurité ;
- 5° description de l'installation, des alentours et de l'environnement ;
- 6° nombre d'employés de l'infrastructure.

Chapitre 2 - Identification, analyse et évaluation des risques

Section 1^{er} - Identification des risques pouvant perturber le fonctionnement de l'infrastructure critique

- 1° Identification des activités de support indispensables au bon fonctionnement de l'infrastructure critique
- 2° Liste des risques pouvant peser sur l'infrastructure critique :
 - a) risques d'origine naturelle, environnementale et sanitaire (par exemple : intempéries graves, inondations et pandémies) ;
 - b) risques d'origine technologique (par exemple : défaillance d'un processus, rupture de l'alimentation en énergie, dysfonctionnement des systèmes informatiques) ;
 - c) risques d'actes malveillants (par exemple : attaque cyber, intrusion, sabotage, attaques terroristes).

Section 2 - Analyse et évaluation des risques identifiés

- 1° Analyse des risques préalablement identifiés :
 - a) analyse des risques suivant l'impact en cas de dysfonctionnement ou de rupture d'une activité de support indispensable au fonctionnement de l'infrastructure critique ;
 - b) analyse des risques suivant l'ampleur de l'impact sur les activités de l'infrastructure en cas de réalisation d'un risque ;
 - c) analyse des risques suivant la probabilité de survenance d'un risque.
- 2° Évaluation des risques préalablement identifiés :
 - a) établissement, sur base des analyses précitées, d'un ordre de priorité au niveau du traitement des risques.

Chapitre 3 - Mesures de réduction des risques et stratégies préventives

Identification des mesures permanentes visant à réduire la probabilité de survenance, respectivement l'impact d'un risque et des mesures graduelles qui peuvent être déclenchées en fonction de la probabilité de réalisation du risque, telles que :

- 1° mesures de contrôle en matière d'accès aux locaux et aux systèmes d'information ;
- 2° systèmes de protection physique ;
- 3° mesures visant à garantir la sécurité informatique ;
- 4° organisation d'exercices de simulation ;
- 5° sensibilisation et formation du personnel.

Chapitre 4 - Dispositif de continuité de l'activité

1° Établissement d'un plan de continuité de l'activité déclenché en cas de réalisation d'un risque :

- a) identification des activités clés ;
- b) processus d'activation du plan ;
- c) rôles et responsabilités des personnes ayant autorité pour la mise en œuvre du plan ;
- d) procédures de communication interne et externe ;
- e) exigences en termes de ressources ;
- f) description des mesures à prendre, par ordre de priorité, pour maîtriser la situation et pour en limiter les conséquences ;
- g) description des mesures en relation avec la continuité des activités de support indispensables au fonctionnement de l'infrastructure ;
- h) processus de désactivation du plan.

2° Organisation à mettre en place pour la gestion d'une crise qui, par sa nature ou son intensité, dépasse le dispositif de continuité de l'activité précité.

* * *

Il est recommandé de procéder périodiquement à une évaluation du plan de sécurité et de continuité de l'activité ou en cas de faits nouveaux justifiant une évaluation en dehors de cette périodicité.

