Institut national de la recherche scientifique

POLITIQUE DE CONTINUITÉ DES ACTIVITÉS ET DE GESTION DES MESURES D'URGENCE

ADOPTION		
INSTANCE	**DATE**	**DÉCISION**
Conseil d'administration	28 septembre 2021	473A-20210928-4130

MODIFICATION(S)		
INSTANCE	**DATE**	**DÉCISION**

RESPONSABLE	Direction générale
CODE	P-13-2021.4

TABLE DES MATIÈRES

PRÉAMBULE

L'Institut national de la recherche scientifique (**INRS**) souhaite maintenir un environnement sécuritaire pour la Communauté INRS ainsi que pour toute personne qui se trouve sur sa propriété. Dans cet esprit, l'INRS s'est doté de plans de mesures d'urgence (**PMU**). La *Politique de continuité des activités et de gestion des mesures d'urgence* (**Politique**) vise à assurer la continuité de ses activités en toutes circonstances et à élaborer une stratégie d'intervention en réponse aux Situations d'urgence et aux cyberincidents qui pourraient survenir à l'INRS.

1. OBJECTIFS

Plus spécifiquement, les objectifs poursuivis par la Politique sont :

a) d'assurer la continuité de ses activités en toutes circonstances, incluant en cas de cyberincident;
b) d'assurer la sécurité de la Communauté INRS et de protéger les biens matériels appartenant à l'INRS en cas de Situation d'urgence;
c) de réduire au minimum les impacts d'une Situation d'urgence ou d'un cyberincident sur les activités de l'INRS;
d) d'établir un cadre de référence en matière de gestion d'une Situation d'urgence;
e) de prévoir une structure organisationnelle et d'identifier les personnes intervenantes chargées de répondre aux Situations d'urgence;
f) de structurer l'élaboration de PMU prévoyant des actions de prévention, de préparation, d'interventions et des mesures de rétablissement à déployer en Situation d'urgence;
g) d'assurer la cohérence des actions posées par l'INRS avec celles des Autorités externes appelées à intervenir en Situation d'urgence;
h) d'inspirer confiance à la Communauté INRS et au public envers l'INRS quant à sa capacité de réagir en Situation d'urgence et de cyberincident;
i) de déterminer les besoins relatifs aux communications afin de veiller à la circulation efficace et coordonnée de l'information en temps opportun;
j) de développer une maîtrise des outils de protection des ressources informationnelles et identifier ses vulnérabilités.

2. DÉFINITIONS

Aux fins d'application de la Politique, les expressions définies revêtent le sens qui leur est donné dans le présent article.

Autorités externes : services d'urgence publics, dont notamment les corps policiers, les services de protection contre les incendies, les services ambulanciers et toute autre entité publique susceptible d'intervenir en cas de Situations d'urgence.

Campus Laval : désigne le lieu où se déroulent les activités du Centre Armand-Frappier Santé Biotechnologie, du Laboratoire national de biologie expérimentale et du Service des immeubles et des équipements.

Cellule de crise et de rétablissement ou CCR : le groupe responsable d'analyser les Situations d'urgence lorsqu'elles se produisent, de formuler une stratégie à adopter, d'établir des orientations ou des directives et de les communiquer à la ou au DMU, à la directrice ou au directeur du Service des communications et des affaires publiques ainsi qu'à la directrice ou au

directeur de cabinet et des relations gouvernementales. Les directeurs de centre peuvent en faire partie lors d'une urgence de niveau élevé.

Centre : le Centre Eau Terre Environnement, le Centre Énergie Matériaux Télécommunications, le Centre Armand-Frappier Santé Biotechnologie ou le Centre Urbanisation Culture Société de l'INRS.

Comité consultatif institutionnel sur les mesures d'urgence ou CCIMU : comité responsable de conseiller le comité de direction en prévention et en préparation des mesures d'urgence.

Comité consultatif local sur les mesures d'urgence ou CCLMU : comité au sein de chacun des Centres et du Campus Laval qui a la responsabilité de voir à l'élaboration, la diffusion et la mise à jour des PMU.

Comité de coordination des communications d'urgence ou CCCU : comité formé des membres du Service des communications et des affaires publiques responsable d'appliquer le plan de communication d'urgence.

Comité de coordination des mesures d'urgence ou CCMU : le comité formé au sein de chacun des Centres et du Campus Laval, responsable d'exercer la coordination de la mise en œuvre du PMU et d'assurer un soutien aux personnes intervenantes.

Comité de la continuité des activités (CCA) : le comité est composé du personnel cadre du Service des ressources matérielles, du Service des ressources informationnelles, du Service des finances, du Service des communications et des affaires publiques, du Service des immeubles et des équipements, du Laboratoire national de biologie expérimentale ainsi que de deux gestionnaires de l'administration de centre et de la conseillère ou du conseiller en optimisation des processus et en gestion des risques.

Communauté INRS : les membres du personnel, incluant le Personnel cadre supérieur, le personnel cadre et le corps professoral, la communauté étudiante, les stagiaires et les stagiaires postdoctoraux de l'INRS.

Directrice ou Directeur des mesures d'urgence ou DMU : la personne nommée par le comité de direction responsable de recevoir les orientations et les directives de la CCR et de les communiquer au CCMU concerné par la Situation d'urgence.

Indice d'aggravation : indicateur complémentaire aux niveaux d'urgence qui permet de déterminer si le site fait face à un risque stable, mineur ou majeur de détérioration de la situation. Cet indicateur se retrouve sur la matrice des niveaux d'urgence et d'aggravation, matrice qui doit être utilisée pour évaluer toute Situation d'urgence qui se présente.

Personnel cadre supérieur : la directrice générale ou le directeur général, la directrice scientifique ou le directeur scientifique, la directrice ou le directeur de l'administration ainsi que la secrétaire générale ou le secrétaire général de l'INRS.

Plan de mesures d'urgence ou PMU : le document mettant en commun des informations visant l'alerte et la mobilisation ainsi que le rôle et les responsabilités de chacune des personnes intervenantes ciblées, et ce, dans les quatre dimensions de la sécurité civile (prévention, préparation, intervention et rétablissement). Les plans de mesures d'urgence incluent des plans particuliers d'intervention qui énumèrent les mesures particulières qui doivent être mises en

œuvre pour assurer la sécurité des personnes et des biens matériels de l'INRS, pour un risque spécifique.

Responsable de la continuité des activités (RCA) : la ou le DMU est implicitement RCA étant donné la description de ses tâches.

Situation d'urgence : tout incident provoquant un impact sur le cours normal du déroulement des activités de l'INRS résultant d'un imprévu, d'un accident, d'un conflit ou d'une attaque, présentant un risque pour la sécurité des personnes ou l'intégrité des biens matériels ou une atteinte à l'image organisationnelle et nécessitant une prise en charge immédiate.

3. CHAMP D'APPLICATION

La Politique s'applique à l'ensemble de la Communauté INRS, aux locataires ainsi qu'à toute personne se trouvant dans un immeuble de l'INRS lors d'une Situation d'urgence ou d'un cyberincident.

4. RESPONSABLE DE L'APPLICATION

La Direction générale est responsable de l'application de la Politique.

5. PRÉVENTION DES MESURES D'URGENCE

La structure organisationnelle de gestion des mesures d'urgence préventives à l'INRS implique les deux comités suivants :
- le Comité consultatif institutionnel sur les mesures d'urgence; et
- le Comité consultatif local sur les mesures d'urgence.

Le CCIMU et le CCLMU sont appelés à mettre en place des mesures par lesquelles l'INRS peut prévenir la survenance de Situations d'urgence, élaborer et diffuser des mesures d'urgence adéquates, réduire les impacts découlant des Situations d'urgences et documenter la gestion des mesures d'urgence.

5.1 COMITÉ CONSULTATIF INSTITUTIONNEL SUR LES MESURES D'URGENCE (CCIMU)

Le CCIMU conseille le comité de direction en matière de gestion de Situation d'urgence.

Plus spécifiquement, en collaboration avec la ou le DMU, le CCIMU :
- effectue la mise à jour de la Politique;
- participe à la mise à jour des PMU, laquelle inclut les plans particuliers d'intervention, de chacun des Centres et du Campus Laval afin de s'assurer qu'ils couvrent l'ensemble de tous les risques actuels et qu'ils sont cohérents avec la Politique et en recommandent l'acceptation au comité de direction;
- recommande au comité de direction des mesures d'atténuation ou d'élimination des impacts et conséquences des risques identifiés;
- voit à la création et au maintien d'un programme d'exercices visant à mettre en application les différentes composantes du PMU et le soumet au comité de direction;

- participe à l'élaboration d'un programme de formation relativement aux PMU élaborés et le soumet au comité de direction;
- participe à l'élaboration d'un programme d'information à l'intention des Autorités externes et le soumet au comité de direction;
- participe à la création et au maintien d'un programme de rétroaction favorisant l'analyse de la réponse et le dépôt de recommandations, tant à l'interne qu'à l'externe, de manière à permettre l'apprentissage à travers les situations vécues et le soumet au comité de direction;
- effectue un rapport annuel adressé au comité de direction et au Conseil faisant état de l'avancement des travaux de chacun des programmes identifiés et des besoins particuliers afin d'assurer l'amélioration du degré de préparation de l'INRS en matière de mesures d'urgence.
- participe à la révision bisannuelle des Situations d'urgence s'étant produites à l'INRS.

Les membres du CCIMU sont les gestionnaires de l'administration des Centres et le Personnel cadre des Services suivants :

- Service des immeubles et des équipements;
- Service des communications et des affaires publiques;
- Service des affaires juridiques;
- Service des ressources informationnelles;
- Service des ressources matérielles;
- Service des ressources humaines;
- Laboratoire national de biologie expérimentale.

Le CCIMU relève du DMU et il peut s'adjoindre d'autres conseillères ou conseillers au besoin.

Le CCIMU se réunit au moins deux fois par année.

5.2 COMITÉ CONSULTATIF LOCAL SUR LES MESURES D'URGENCE (CCLMU)

Chaque CCLMU exerce les responsabilités suivantes :

- voir à l'élaboration, la diffusion et la mise à jour du PMU;
- établir les mécanismes de coopération avec les Autorités externes (services d'incendies, services policiers, services ambulanciers, sécurité civile, services sociaux, services de location, etc.);
- s'assurer de fournir aux différentes personnes intervenantes la formation requise par le PMU;
- s'assurer de l'application des programmes relatifs aux mesures d'urgence;
- faire rapport de ses activités au CCIMU et au comité de santé et sécurité du Centre concerné ou du Campus Laval;
- sur une base bisannuelle (1er juin et 1er décembre), élaborer un rapport relatant les Situations d'urgence auxquelles les Centres ou le Campus Laval ont dû faire face;
- faire des recommandations au CCIMU.

Chaque CCLMU se réunit minimalement deux fois par année financière ou davantage au besoin.

Chaque CCLMU est présidé par la personne responsable du CCMU concerné, qui en désigne les membres.

5.3 PLANS DES MESURES D'URGENCE (PMU)

5.3.1 Élaboration des PMU

Chacun des CCLMU est tenu d'élaborer et de mettre à jour annuellement le PMU pour son Centre ou le Campus Laval, en collaboration avec le CCIMU.

Le PMU doit rencontrer les principes directeurs suivants :

- permettre de cerner les Situations d'urgence susceptibles de se produire dans l'environnement interne ou externe du Centre concerné ou du Campus Laval et d'inclure des plans particuliers d'intervention adaptés aux différentes Situations préalablement identifiées;
- tenir compte des quatre dimensions de la sécurité civile : « prévention », « préparation », « intervention » et « rétablissement » pour préserver la vie et la sécurité des personnes et leur apporter secours, sauvegarder les biens matériels ou atténuer les effets d'une Situation d'urgence;
- être concis et bien structuré et comporter suffisamment de détails pour assurer un accès rapide à de l'information critique lors d'une Situation d'urgence;
- prévoir un plan de communication d'urgence visant à informer la Communauté INRS et le public si requis afin de maintenir un climat de confiance.
- être facilement accessible et connu de la Communauté INRS appelée à jouer un rôle en cas de Situation d'urgence.

5.3.2 Diffusion des PMU

Le CCMU est responsable de faire connaître le PMU du Centre concerné ou du Campus Laval à la Communauté INRS susceptible d'être impliquée dans sa mise en œuvre, de même qu'aux services d'urgences des Autorités externes lorsque requis. À cette fin, le CCMU met en place des programmes spécifiques d'exercices et de formation destinés aux membres de la Communauté INRS.

5.3.3 Mise à jour des PMU

Les PMU sont mis à jour annuellement.

6. CONTINUITÉ DES ACTIVITÉS

6.1 PLAN DE CONTINUITÉ DES ACTIVITÉS

6.1.1 Description

Le plan de continuité des activités identifie les processus prioritaires, les ressources indispensables et les stratégies de protection pour le maintien des activités essentielles de l'INRS ou leur reprise à brève échéance, et ce, en toutes circonstances.

Le Formulaire en cas de Situations d'urgence et de cyberincident, joint en Annexe 4, permet à la ou au DMU, en collaboration avec les CCMU :

- d'établir les impacts sur les ressources humaines, matérielles, informationnelles, immobilières, technologiques, de même qu'à l'égard des fournisseurs externes;

- de définir les stratégies de continuité à mettre en œuvre pour prévenir ou pallier les risques; et
- d'évaluer le temps nécessaire à la reprise des activités.

Le plan de continuité des activités inclut un plan de sauvegarde des données. Advenant une Situation d'urgence ou un cyberincident causant l'arrêt ou la dégradation d'un service, celui-ci doit être consulté auprès de la ou du DMU.

Les systèmes principaux, les fonctions des activités essentielles, les durées de reprise et les différentes stratégies de relève à mettre en place sont identifiés au plan de continuité des activités.

6.1.2 Contrôle de l'efficacité

La ou le DMU valide l'efficacité du plan de continuité des activités sur une base régulière, tant sur une base théorique que par le biais de simulations de sinistres fictifs.

6.1.3 Maintenance

Le plan de continuité des activités demeure opérationnel en tout temps et est maintenu à jour par la ou le DMU lorsque surviennent des changements susceptibles de l'impacter. À ces fins, un programme de gestion des changements identifie les éléments déclencheurs à prendre en compte, dont notamment :

- les changements organisationnels (mission, allocations budgétaires et autres);
- les changements externes (lois et règlements, clientèles, fournisseurs et autres).

Le Service des ressources informationnelles veille à l'administration des sauvegardes de données.

6.1.4 Assurance

L'INRS acquiert et maintient une assurance en cybersécurité.

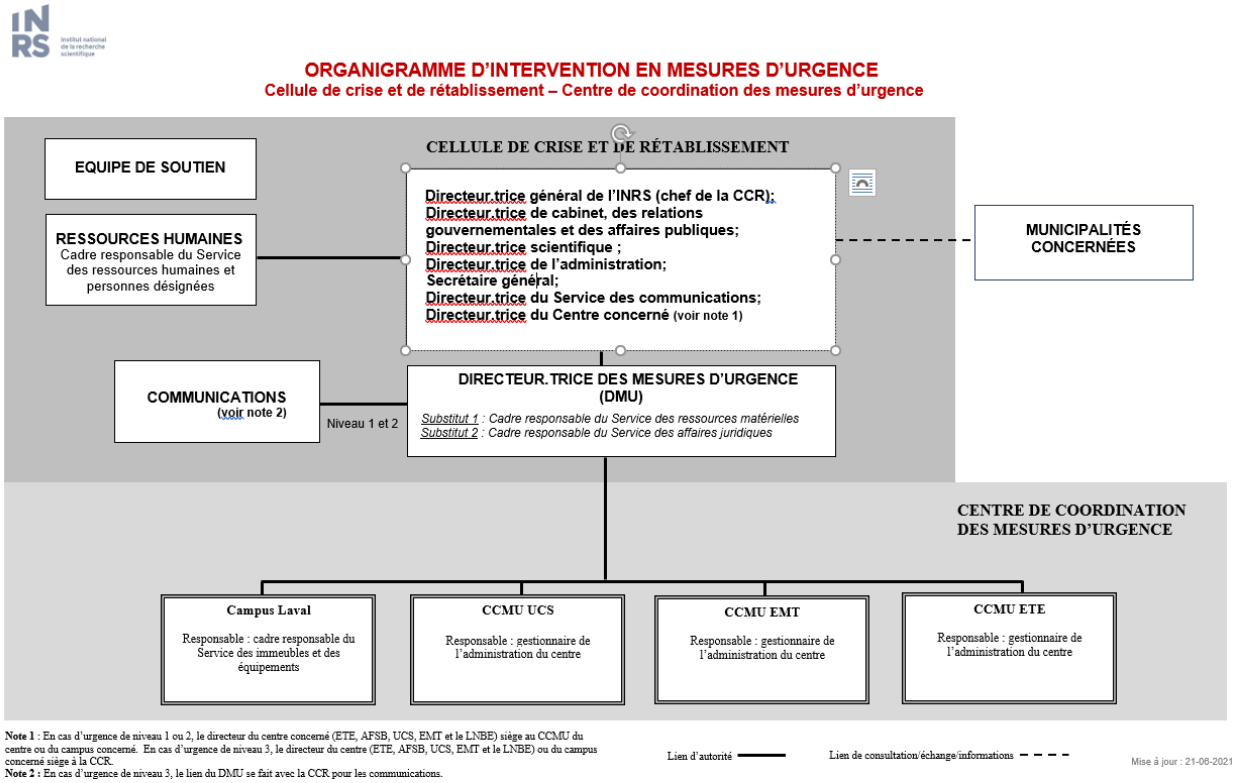
7. GESTION DES MESURES D'URGENCE

La structure organisationnelle de gestion des mesures d'urgence en cas de Situations d'urgence implique les quatre entités suivantes, qui sont appelées à se mobiliser pour réagir en cas de Situations d'urgence. Ces entités doivent parfois coordonner leurs interventions avec celles des Autorités externes :

- la Cellule de crise et de rétablissement (CCR);
- la Directrice ou le Directeur des mesures d'urgence (DMU);
- les Comités de coordination des mesures d'urgence (CCMU);
- le Comité de coordination des communications d'urgence (CCCU).

7.1 COMPOSITION ET ORGANIGRAMME

La composition de ces entités et leur organisation sont exposées à l'organigramme suivant :



7.2 RÔLES ET RESPONSABILITÉS

7.2.1 Cellule de crise et de rétablissement (CCR)

Sous l'autorité de la Direction générale, la CCR se réunit en fonction des besoins ou dès qu'une Urgence de niveau 3 est imminente ou survient (physiquement, par téléphone ou par tout autre moyen ne faisant pas appel au système compromis).

La CCR assume les responsabilités suivantes :

- prendre acte du résumé de la Situation d'urgence ou du cyberincident, présenté par la ou le DMU, lequel inclut toute information recueillie lors de l'évaluation;
- analyser la situation et ses effets internes et externes;
- poser un diagnostic;
- adopter une stratégie de support au déploiement d'un PMU; et
- donner des orientations et directives spécifiques à la ou au DMU, lesquelles sont aussitôt transmises au CCMU concerné ainsi qu'à la directrice ou au directeur du Service des ressources informationnelles (**DRI**), le cas échéant;
- participer à l'élaboration du rapport de rétroaction.

Les membres du CCR sont le Personnel cadre supérieur, la ou le DMU, la directrice ou le directeur de cabinet et des relations gouvernementales et la directrice ou le directeur du Service des communications et des affaires publiques.

La Direction générale assume la responsabilité de la CCR et s'assure que des personnes substituts soient désignées pour participer au besoin à la CCR.

En cas d'urgence de niveau 3, la direction du Centre concerné participe à la CCR. En cas de cyberincident, la ou le DRI participe à la CCR.

7.2.2 Directrice ou Directeur des mesures d'urgence (DMU)

La ou le DMU agit à titre d'intermédiaire entre la CCR et la personne responsable du CCMU concerné. Cette personne obtient toutes les informations requises sur la Situation d'urgence et en informe la personne responsable de la CCR. Elle apporte également le support nécessaire afin que le CCMU concerné mette en œuvre les orientations et les directives de la CCR. Ses principales responsabilités consistent à :

- répondre aux appels de la personne responsable du CCMU concerné;
- conjointement avec la personne responsable du CCMU concerné, déterminer la nature et le niveau de la Situation d'urgence et en suivre l'évolution;
- demander l'activation du CCMU concerné si nécessaire;
- informer le comité de direction et le Service des communications et des affaires publiques et selon le niveau d'urgence, informer la CCR;
- s'assurer, lorsque requis, que les assureurs soient contactés;
- participer à l'élaboration d'un plan de rétablissement;
- assurer un suivi post-événement;
- rendre compte à la CCR lorsque requis;
- documenter les interventions d'une Situation d'urgence dans un journal des opérations;
- s'assurer de l'élaboration, de la mise à niveau et du maintien d'un PMU pour chaque Centre concerné et pour le Campus Laval;
- coordonner la mise en place du plan de continuité des activités et veiller à sa mise à jour.

7.2.3 Comité de coordination des mesures d'urgence (CCMU)

Sous l'autorité de la personne responsable du CCMU, le CCMU voit au déploiement du PMU et à la mise en œuvre des orientations et directives de la CCR. Il est responsable de la mise en application des mesures prévues au PMU et supervise les actions dans la mise en œuvre du plan particulier d'intervention. Il s'en remet aux orientations et décisions de la ou du DMU lorsque la CCR est activée.

Le CCMU se réunit à l'endroit désigné et adapté comme lieu de coordination au PMU.

La personne responsable du CCMU du Campus Laval est la directrice ou le directeur du Service des immeubles et des équipements. Le CCMU du Campus Laval veille aussi à la sécurité du Laboratoire national de biologie expérimentale de même qu'à celle des locataires de l'INRS sur le Campus Laval. Les responsables des CCMU des Centres sont les gestionnaires de l'administration du Centre.

7.2.4 Équipes de réponse à une Situation d'urgence ou à un cyberincident

7.2.4.1 En cas de Situation d'urgence

L'équipe de réponse à une Situation d'urgence est déterminée par chacun des Centres. Chacun des CCMU détient des procédures particulières d'intervention et travaille en collaboration avec la ou le DMU.

7.2.4.2 En cas de cyberincident

L'équipe de réponse aux cyberincidents (**ÉRC**) est constituée des membres du personnel du Service des ressources informationnelles et la liste des coordonnées et responsabilités de ces personnes est détenue par la ou le DRI et la ou le DMU.

7.2.5 Comité de coordination des communications d'urgence (CCCU)

Sous l'autorité du Service des communications et des affaires publiques, le CCCU élabore un plan de communication d'urgence et voit à sa mise en œuvre. Le CCCU est responsable d'informer les membres de la Communauté INRS de la survenance et de l'évolution d'une Situation d'urgence, ainsi que de mettre en œuvre les mesures utiles à la préservation de l'intégrité de l'image et de la réputation de l'INRS. Le CCCU est composé des personnes désignées par le Service des communications et des affaires publiques.

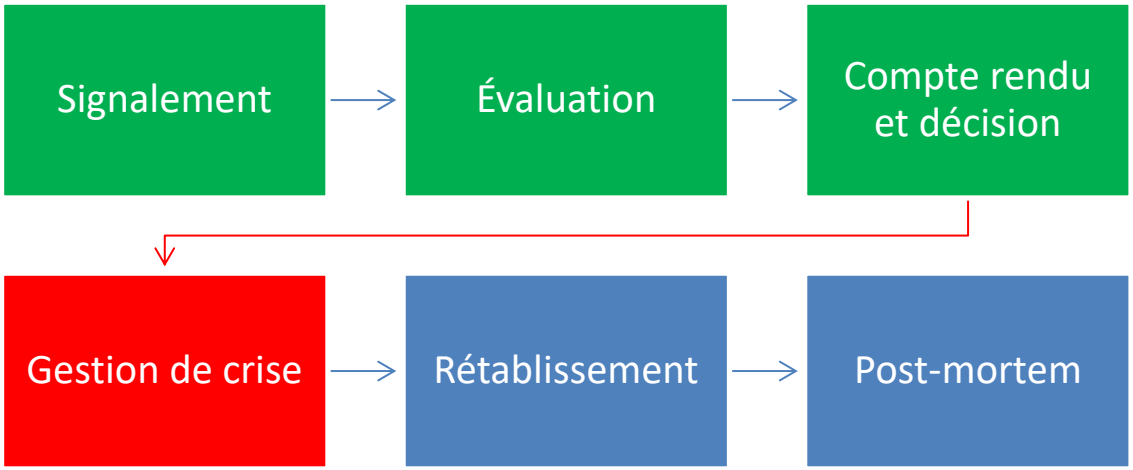
Lors d'une Situation d'urgence, le Centre concerné ou le Campus Laval peut communiquer avec les membres de la Communauté INRS concernés pour émettre des directives visant à les informer de la Situation d'urgence, à assurer leur sécurité ou à les rassurer.

Le Service des communications et des affaires publiques peut également communiquer avec les membres de la Communauté INRS pour les informer de l'évolution ou des détails relatifs à une Situation d'urgence. Afin d'éviter la multiplication des messages, les communiqués internes peuvent également inclure des directives aux membres de la Communauté INRS concernés, dans la mesure où ils sont préalablement validés par le CCMU concerné.

7.2.6 Service des ressources informationnelles

La ou le DRI est responsable de la sécurité de l'information et de la gestion des cyberincident.

7.3 PROCÉDURE DE RÉPONSE À UNE SITUATION D'URGENCE OU À UN CYBERINCIDENT



En cas de cyberincident, les articles 7.3.1 à 7.3.5 sont remplacés par la *Procédure de réponse à un cyberincident* jointe à l'Annexe 1.

7.3.1 Signalement

Le signalement peut venir de diverses sources. Il peut être anticipé ou se produire soudainement.

Lorsque la Situation d'urgence peut être anticipée (ex : pandémie), la CCR se réunira afin d'anticiper les impacts sur les ressources de l'INRS, déterminer les actions à poser et désigner les personnes pour le faire en fonction des actions et des communications nécessaires à la protection des ressources et des processus à protéger.

Lorsque la Situation d'urgence est soudaine (explosion, feu, etc.), les CCMU concernés envoient un message d'urgence à l'aide des outils de messagerie de masse disponibles, afin de coordonner les actions à prendre dépendamment de la situation.

7.3.2 Évaluation du niveau d'urgence et ouverture d'un CCMU

L'évaluation d'une Situation d'urgence se fait obligatoirement en trois étapes :
1. déterminer le niveau d'urgence de la Situation d'urgence;
2. déterminer le niveau de risque d'aggravation de la Situation d'urgence;
3. déterminer si un CCMU doit être ouvert ou non.

7.3.2.1 Niveaux d'urgence

Les indicateurs de niveau 1, 2 ou 3 permettent d'évaluer et de qualifier la gravité d'une Situation d'urgence. Ces niveaux sont déterminés à partir des critères énoncés à la *Matrice des niveaux d'urgence et d'aggravation* (Annexe 2). Cette matrice doit être utilisée pour toute Situation d'urgence qui se présente. Dans le doute, l'indice supérieur doit être utilisé.

7.3.2.2 Indices d'aggravation

À l'aide de la Matrice des niveaux d'urgence et d'aggravation (Annexe 2), cet indice permet de déterminer quel est le risque de détérioration de la Situation, dans un délai plus ou moins long, en fonction des constats faits par les services compétents. Ici encore, dans le doute, l'indice supérieur doit être appliqué.

7.3.2.3 Risque stable

La Situation d'urgence est sous contrôle et ne risque pas de s'aggraver.

7.3.2.4 Risque d'aggravation mineur

Bien que généralement maîtrisée, la Situation d'urgence n'est pas complètement sous contrôle et présente un certain risque d'aggravation.

7.3.2.5 Risque d'aggravation majeur

La Situation d'urgence est hors contrôle et présente un risque certain d'aggravation.

7.3.3 Compte rendu et décision de l'ouverture d'un CCMU

Selon l'évaluation du niveau d'urgence, différentes actions doivent être posées pour gérer la Situation d'urgence. La décision d'ouverture d'un CCMU est prise à l'aide de la Fiche d'aide à la décision jointe à l'Annexe 3.

7.3.4 Gestion de crise

Lors d'un incident d'urgence élevée, la CCR est avisée et impliquée dans la suite des opérations. Son rôle et ses responsabilités sont prévus à l'article 7.2.1.

7.3.5 Rétablissement

Lorsqu'une Situation d'urgence est maîtrisée, le retour au cours normal des activités de l'INRS est amorcé, et ce, même s'il est impossible de prévoir si ce retour est définitif ou temporaire. Il faut donc mettre en œuvre les mesures de rétablissement prévues au PMU, lesquelles concernent notamment :

- les aspects humains, logistiques et financiers de la reprise des activités;
- les priorités pour la reprise des activités et la séquence des actions à entreprendre.

7.3.6 Post-mortem

Cette étape vise à revenir sur l'événement, les causes à l'origine de la Situation d'urgence ou du cyberincident et l'efficacité de la réponse face à celui-ci.

Dans un premier temps, une rencontre a lieu entre le CCMU et la ou le DMU afin d'effectuer un retour sur la Situation d'urgence de façon à :

- identifier les vulnérabilités à l'origine de l'incident : dresser la liste de celles qui ont été corrigées et de celles qui devront l'être, en incluant un échéancier de réalisation;
- établir des solutions et mécanismes visant à empêcher qu'un nouvel événement semblable ne se reproduise dans l'avenir;
- mettre de l'avant des solutions pour améliorer le processus de réponse advenant une prochaine Situation d'urgence;
- consigner l'événement dans le registre (DMU) et le Formulaire en cas de Situations d'urgence et de cyberincident (Annexe 4) à cette fin, ainsi que les solutions à mettre de l'avant;
- réviser le projet de rapport avec les membres du CCMU.

S'il s'agit d'un cyberincident, l'ÉRC ainsi que la ou le DRI participe à la rencontre précitée.

Lors d'une deuxième phase, la ou le DRI et la ou le DMU rédigent un rapport synthétisant les éléments identifiés lors de la première phase. La gestion de crise et les problèmes rencontrés sont aussi évalués afin d'identifier les bons éléments et les correctifs à apporter aux éléments à améliorer. Ce rapport est ensuite soumis pour révision aux membres de la CCR et la version finale est présentée par la ou le DMU au comité d'audit.

7.3.7 Fin de la situation d'urgence ou du cyberincident

À la suite du rétablissement du cours normal des activités de l'INRS, la fin de la Situation d'urgence est déclarée par la personne responsable du CCMU, suivant une concertation avec la ou le DMU.

8. COORDINATION AVEC LES AUTORITÉS EXTERNES

8.1 PRISE EN CHARGE PAR LES AUTORITÉS EXTERNES

Lorsque les Autorités externes interviennent, elles prennent en charge le périmètre d'intervention qu'elles ont déterminé. L'INRS s'en remet alors aux directives de ces dernières et joue un rôle de support auprès de ces Autorités externes. À l'extérieur de ce périmètre d'intervention, la responsabilité du site est assumée par le CCMU concerné, en collaboration avec les Autorités externes.

8.2 FIN DE L'INTERVENTION DES AUTORITÉS EXTERNES

La fin de l'intervention des Autorités externes survient au moment où, en collaboration avec l'INRS, les Autorités externes décident de se démobiliser et que l'INRS reprend le contrôle de la Situation d'urgence et passe en mode rétablissement.

9. MISE À JOUR

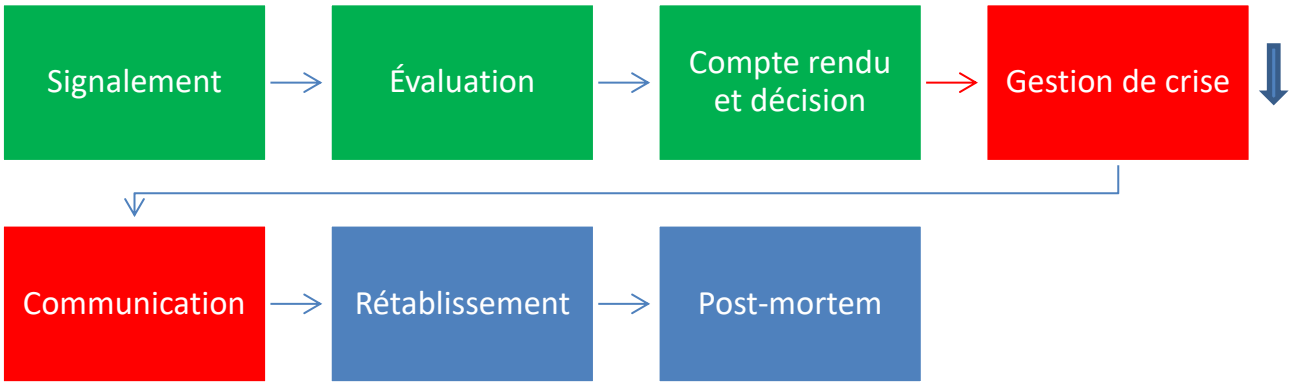
La Politique est mise à jour minimalement aux trois ans ou au besoin.

Quant aux annexes 2, 3 et 4 de la Politique, celles-ci sont misent à jour, en fonction des besoins par la personne occupant la fonction de DMU.

10. DISPOSITIONS FINALES

La Politique entre en vigueur au moment de son adoption par le conseil d'administration de l'INRS.

ANNEXE 1 - PROCÉDURE DE RÉPONSE À UN CYBERINCIDENT



SIGNALEMENT

Le signalement peut provenir de diverses sources. Il peut venir d'une personne utilisant les ressources informationnelles de l'INRS, son réseau ou de signaux d'alarme du système de surveillance des activités du réseau de l'INRS.

En cas de signalement, les étapes suivantes sont enclenchées :
- prendre connaissance du signalement;
- isoler les équipements compromis du reste du réseau :
  - débrancher du système toutes les composantes affectées par le cyberincident;
  - prendre une image du système;
- transmettre un message de mesures d'urgence à la Communauté INRS (DMU) et assurer des rétroactions régulières concernant l'état de la situation.

ÉVALUATION

Une fois le cyberincident signalé, l'ÉRC détermine les causes et les conséquences du cyberincident. L'évaluation complète nécessite les actions suivantes :
- établir la liste des systèmes et comptes affectés;
- déterminer si des renseignements personnels ont été compromis;
- évaluer le temps nécessaire à la reprise des activités;
- conserver toute preuve pour l'équipe externe mandatée par la compagnie d'assurances.

COMPTE RENDU ET DÉCISION

Le niveau d'impact que représente l'événement détermine la réponse au cyberincident. Tout cyberincident impliquant la compromission d'un renseignement personnel est considéré comme ayant un impact élevé. L'ÉRC détermine le niveau d'impact à l'aide de ses premières constatations. Voici les trois niveaux possibles et les actions à poser, le cas échéant :

IMPACT	DESCRIPTION	ACTIONS À PRENDRE
Faible (niveau 1)	– aucun renseignement personnel compromis; – interruption des activités faible ou limitée.	– remplir le Formulaire en cas de Situations d'urgence et de cyberincident (Annexe 4); – aviser la Communauté INRS du prompt rétablissement du service, s'il a été interrompu (DMU); – continuer à l'étape Rétablissement (DMU);
Modéré (niveau 2)	– aucun renseignement personnel compromis; – interruption des activités partielle ou complète avec un délai de reprise estimées de moins de 24 heures.	
Élevé (niveau 3)	– renseignements personnels compromis; – interruption des activités importante ou complète, avec un délai de reprise de plus de 24 heures.	– contacter les assurances (responsable des assurances au Service des ressources matérielles) – contacter les firmes identifiées par l'assurance (DRI et le Service des affaires juridiques pour les consultants juridiques) – ouvrir la CCR; – remplir le Formulaire en cas de Situations d'urgence et de cyberincident (DMU et DRI); – aviser la Communauté INRS des derniers développements et de la prolongation de l'interruption de services (DMU); – continuer à l'étape de Gestion de crise.

GESTION DE CRISE

Dans le cas d'un cyberincident à impact élevé, la CCR est avisée et impliquée dans la suite des opérations. Son rôle et ses responsabilités sont prévus à l'article 7.2.1

COMMUNICATIONS ET NOTIFICATIONS

Si des données personnelles sont compromises, un sous-comité de communication d'urgence est formé pour coordonner la communication de l'information sensible. Celle-ci sera fournie par l'ÉRC. Le sous-comité est composé des membres suivants :

- les fournisseurs de services mandatés par l'assurance;
- le Service des affaires juridiques;
- le Service des communications et des affaires publiques.

RÉTABLISSEMENT

L'étape de rétablissement vise à rétablir les services touchés, dans les meilleurs délais, afin d'assurer la reprise des activités. Selon la situation, le rétablissement peut impliquer des services techniques externes fournis par l'assurance. Le rétablissement doit veiller, s'il y a lieu, à préserver les preuves. De plus, le rétablissement doit être fait prudemment afin de veiller à ne pas recréer le problème (ex. : réinfection de virus). L'ÉRC effectue les étapes suivantes :

- corriger le problème, avec l'aide des ressources techniques fournies par l'assurance si celle-ci a été impliquée;
- réinstaller le système de zéro, les systèmes de sécurité, de même que les données à partir des dernières sauvegardes;
- analyser les privilèges des comptes ayant pu être affectés;
- remettre le système en ligne.

ANNEXE 2 – MATRICE DES NIVEAUX D'URENCE ET D'AGGRAVATION

MATRICE DES NIVEAUX D'URGENCE ET D'AGGRAVATION

Version: 2015/05/26

Événement: _____

Date: ___ / ___ / ___ Heure: ___ : ___ Complété par: _____

ÉTAPE 1 Déterminer le niveau d'urgence

	Niveau 1	Niveau 2	Niveau 3	Commentaire
Blessés (nombre)	0 - 5 ☐	6 - 10 ☐	11 + ou mortalité ☐	
Dommages (bâtiment)	Mobilier, esthétique, etc. ☐	Systèmes vitaux du bâtiment ☐	Structurels ☐	
Perturbation des activités	0 – 24 hrs ☐	2 – 7 jours ☐	8 jours + ☐	
Rayonnement (image de l'INRS)	Site ☐	INRS ☐		
Actions à prendre	L'événement peut être géré localement Avis au DMU par le chef du CCMU concerné Avis à la direction des communications par le DMU	L'événement peut être géré localement Avis au DMU par le chef du CCMU concerné Avis à la direction des communications par le DMU	**LA CCR est activée** **Avis au DMU par le chef du CCMU concerné** **Avis à la direction des communications par le DMU**	

Appliquez le niveau d'indicateur le plus élevé

ÉTAPE 2 En collaboration avec le(s) service(s) compétent(s) (police, pompiers, service interne, etc.), déterminer le risque d'aggravation de la situation:

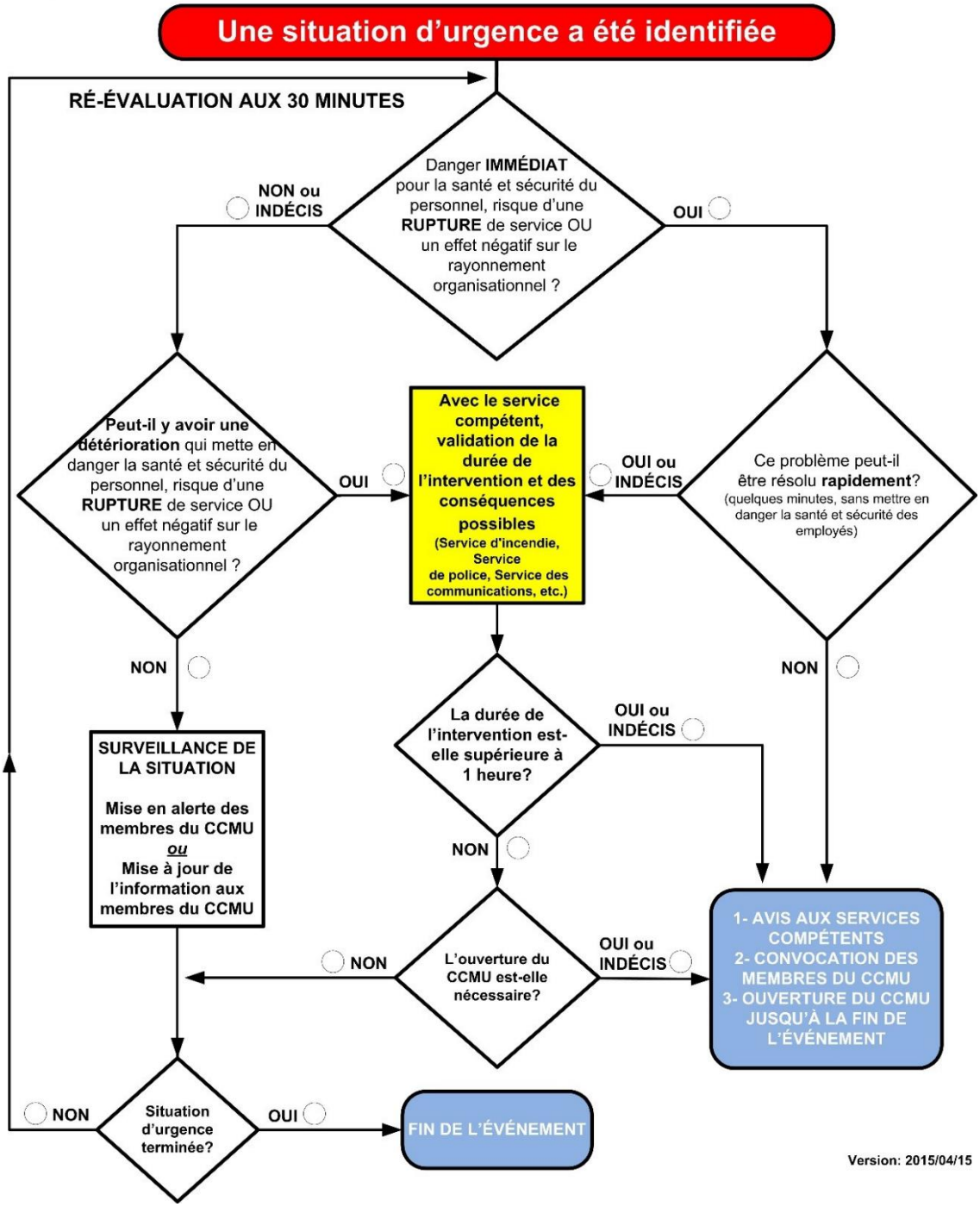
Stable ☐	Mineur ☐	Majeur ☐	
La Situation d'urgence est sous contrôle et ne risque pas de s'aggraver	Bien que généralement maîtrisée, la Situation d'urgence n'est pas complètement sous contrôle et présente un certain risque d'aggravation	La Situation d'urgence est hors contrôle et présente un risque certain d'aggravation	

ANNEXE 3 – FICHE D'AIDE À LA DÉCISION

OUVERTURE D'UN CCMU - FICHE D'AIDE À LA DÉCISION

Événement: _____ Date: ____ / ____ / ____ Heure: ____:____

Complétée par: _____



ANNEXE 4 – FORMULAIRE EN CAS DE SITUATION D'URGENCE ET DE CYBERINCIDENT

FORMULAIRE EN CAS DE SITUATION D'URGENCE ET DE CYBERINCIDENT			
Section I - Description de la Situation d'urgence ou du cyberincident			
1 - Description de l'incident			
2 - Nom de la personne ayant signalé l'incident			
3 - Lieu de l'incident			
4 - Date de l'incident			
5 - Description détaillée de l'incident			
6 - Données personnelles compromises? (Si oui, notifier la CCR)			
7 - UBR ouvert pour collecte de dépenses			
8 - Appel à l'assurance (demander au cadre responsable du Service des ressources matérielles et à la personne responsable des assurances)			
9 - Avocat.e.s contacté.e.s par l'assurance			
10 - Firme spécialisée mandatée par l'assurance			
11 - Comptes bancaires compromis? Si oui, communications avec les institutions bancaires.			
Section II - Ressources affectées			
Ressources	**Oui/nom de la ressource**	**Description si oui (blessés, bris matériel, etc.)**	
Ressources humaines			
Ressources immobilières (locaux)			
Ressources informationnelles			
Ressources technologiques			
Ressources matérielles			
Fournisseurs externes			
Locataires			
Autres ressources			
Section III - Consultants et fournisseurs d'appoint			
Type de Consultants	**Nom**	**Téléphone**	**Adresse internet**
Assurances			
Avocat.e.s contacté.e.s par l'assurance			
Firmes externes : location de génératrices, refroidisseurs, agence de sécurité…			
Consultant.e.s informatique			
Section IV - Description détaillée de l'attaque - vulnérabilité exploitée ayant permis l'infiltration du réseau			

FORMULAIRE EN CAS DE SITUATION D'URGENCE ET DE CYBERINCIDENT (suite)

Section V - Processus critiques affectés

Processus	Centre service	Oui/nom de la ressource	Si oui, solution préventive ou solution palliative?
Coordonner et appliquer les mesures d'urgence	Centres/SIE		
Assurer l'accès aux locaux et aux installations (Sécurité CNESST)	Centres/SIE		
Gestion de la mécanique du bâtiment (électricité, génératrices, aération, climatisation, détection fuite de gaz, etc.)	Centres/SIE		
Gestion des bourses (demande d'inscription et demande de rémunération)	Centres		
Renouvellement des contrats	Centres		
Réception des commandes	Centres		
Faire le suivi auprès du corps professoral et des client.e.s	LNBE		
Approvisionner le centre en matériel et services			
Gérer l'inventaire			
Maintien de l'environnement des animaux			
Gérer les relations avec les médias (rédiger et publier les communiqués de presse)	Communications		
Gérer les communications internes			
Gérer la mise à jour du site Web			
Gérer les médias sociaux			
Gestion des bourses (demandes d'admission, d'inscriptions et d'abandons)	Service des études et de la vie étudiante		
Gestion des bourses (vérification et paiement des bourses)	Finances		
Traiter les comptes à payer en urgence			
Dépôt des demandes de subventions (selon les règlements de l'organisme subventionnaire)	Service à la recherche		
Traiter la paie	Ressources humaines		
Offrir des conseils juridiques (conseil, opinion, etc.)	Service juridique		
Assurer le fonctionnement des instances	Secrétariat général		