



Gouvernement
du Canada

Government
of Canada

LIGNE DIRECTRICE CANADIENNE SUR LA BIOSÉCURITÉ

ÉLABORATION D'UN PLAN DE BIOSÛRETÉ EXHAUSTIF



Canada

Ligne directrice canadienne sur la biosécurité : Élaboration d'un plan de biosûreté exhaustif est disponible sur Internet à l'adresse suivante :
<http://normescanadiennesbiosecurite.collaboration.gc.ca/>

Also available in English under the title:
Canadian Biosafety Guideline: Developing a Comprehensive Biosecurity Plan

Pour obtenir des copies supplémentaires, veuillez communiquer avec :

Agence de la santé publique du Canada
100 chemin Colonnade
Ottawa (Ontario) K1A 0K9
Tél. : 613-957-1779
Téléc. : 613-941-0596
Courriel d'ASPC : PHAC.standards-normes.ASPC@canada.ca
Courriel d'ACIA : standardsnormes@inspection.gc.ca

On peut obtenir, sur demande, la présente publication en formats de substitution.

© Sa Majesté la Reine du chef du Canada, représentée par la ministre de la Santé et la ministre de l'Agriculture et de l'Agroalimentaire, 2016

Date de publication : juin 2016

La présente publication peut être reproduite sans autorisation pour usage personnel ou interne seulement, dans la mesure où la source est indiquée en entier.

Cat. : HP45-12/2016F-PDF
ISBN : 978-0-660-05675-3
No de publication : 160077

TABLE DES MATIÈRES

PRÉFACE	iv
ABRÉVIATIONS ET ACRONYMES	vi
CHAPITRE 1 - INTRODUCTION	2
1.1 Portée	2
1.2 Aperçu	3
1.3 Utilisation de la Ligne directrice canadienne sur la biosécurité : Élaboration d'un plan de biosûreté exhaustif	3
CHAPITRE 2 - POUR COMMENCER	6
2.1 Rôles et responsabilités	6
2.2 Évaluation des risques de biosûreté	7
2.3 Élaboration du plan de biosûreté	8
CHAPITRE 3 - SÉCURITÉ PHYSIQUE	12
3.1 Barrières physiques et protection graduelle	12
3.2 Mesures de contrôle d'accès	14
3.3 Détection des accès non autorisés et des tentatives d'accès	21
3.4 Considérations d'ordre opérationnel liées au contrôle d'accès	25
CHAPITRE 4 - COMPÉTENCE ET FIABILITÉ DU PERSONNEL	34
4.1 Vérification de la compétence et de la fiabilité	34
4.2 Programme d'évaluation de la fiabilité continue	37
4.3 Habilitation de sécurité en vertu de la LAPHT	38
CHAPITRE 5 - RESPONSABILITÉ À L'ÉGARD DES AGENTS PATHOGÈNES ET DES TOXINES, ET GESTION DE L'INVENTAIRE	42
5.1 Responsabilité à l'égard des agents pathogènes et des toxines	42
5.2 Inventaires et gestion de l'inventaire	43
5.3 Sécurité durant le déplacement et le transport	45
CHAPITRE 6 - INTERVENTION EN CAS D'INCIDENT ET D'URGENCE	50
6.1 Déclaration des incidents	50
6.2 Planification des interventions en cas d'incident	51
6.3 Enquête sur les incidents	53
CHAPITRE 7 - GESTION ET SÉCURITÉ DE L'INFORMATION	56
7.1 Ressources en matière d'information	56
7.2 Classification des renseignements	57
7.3 Sécurité des renseignements	57
CHAPITRE 8 - MISE EN ŒUVRE, ÉVALUATION ET AMÉLIORATION DU PLAN DE BIOSÛRETÉ	68
8.1 Formation	68
8.2 Entretien et vérification des systèmes de sécurité	70
8.3 Évaluation et amélioration continue du plan de biosûreté	70
CHAPITRE 9 - GLOSSAIRE	74
CHAPITRE 10 - RESSOURCES	84
10.1 Ressources générales	84
10.2 Lois du gouvernement du Canada	85

LISTE DES FIGURES

Figure 3-1 : Exemple de zones de protection graduelle dans une installation.	13
Figure 4-1 : Situations où une Habilitation de sécurité en vertu de la LAPHT délivrée par l'ASPC est exigée.	39

LISTE DES TABLEAUX

Tableau3-1 : Aperçu des mesures de contrôle d'accès et des points à prendre en considération pour leur sélection et leur mise en place.	16
Tableau 3-2 : Éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté dans une zone de NC2, de NC3 et d'ABCSE.	20
Tableau3-3 : Résumé des systèmes de détection d'intrusion.	23
Tableau4-1 : Éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté associés à la compétence et à la fiabilité du personnel dans une zone de NC2, de NC3 et d'ABCSE.	35
Tableau5-1 : Éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté associés à la responsabilisation à l'égard d'agents pathogènes et de toxines dans une zone de NC2, de NC3 et d'ABCSE.	43
Tableau5-2 : Éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté associés à la gestion de l'inventaire dans une zone de NC2, de NC3 et d'ABCSE.	45
Tableau 6-1 : Cinq éléments clés pour assurer le succès d'un plan d'intervention en cas d'incident.	51
Tableau 6-2 : Éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté associés aux interventions en cas d'incidents et d'urgences dans une zone de NC2, de NC3 et d'ABCSE.	52
Tableau7-1 : Éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté liés à la sécurité des renseignements dans un NC2, un NC3 et une zone d'ABCSE.	59



PRÉFACE



PRÉFACE

Les *Lignes directrices canadiennes sur la biosécurité* ont été élaborées conjointement par l'Agence de la santé publique du Canada (ASPC) et par l'Agence canadienne d'inspection des aliments (ACIA) dans le cadre d'une série de documents d'orientation, toujours en évolution, portant sur le thème de la biosécurité et de la biosûreté.

Au Canada, la plupart des installations où on manipule ou entrepose des agents pathogènes humains, des agents pathogènes d'animaux terrestres ou des toxines sont régies par l'ASPC et l'ACIA en vertu de la *Loi sur les agents pathogènes humains et les toxines* (LAPHT), le *Règlement sur les agents pathogènes humains et les toxines* (RAPHT), la *Loi sur la santé des animaux* (LSA) et le *Règlement sur la santé des animaux* (RSA). Les installations réglementées sont tenues d'élaborer et de tenir à jour un plan de biosûreté, conformément aux exigences énoncées dans la *Norme canadienne sur la biosécurité* (NCB), 2^e édition, 2015. Le *Guide canadien de la biosécurité* (GCB), 2^e édition vise à offrir aux différents intervenants un soutien et des conseils sur la façon d'effectuer des évaluations des risques de biosûreté et sur les éléments de base d'un plan de biosûreté solide afin de gérer de façon appropriée les risques liés aux agents pathogènes et aux toxines qu'ils ont en leur possession. La ligne directrice *Élaboration d'un plan de biosûreté exhaustif* précise un certain nombre de thèmes de biosûreté présentés dans le GCB et sert de ressource aux intervenants qui veulent obtenir des renseignements et des directives supplémentaires pour établir un plan de biosûreté plus solide et plus détaillé.

La ligne directrice *Élaboration d'un plan de biosûreté exhaustif* est un document en constante évolution qui fait continuellement l'objet d'améliorations. L'ASPC et l'ACIA acceptent volontiers les commentaires, les clarifications et les suggestions afin de les intégrer aux versions ultérieures du présent document d'orientation. À cette fin, veuillez faire parvenir l'information accompagnée de références (s'il y a lieu) pour assurer l'amélioration continue de la ligne directrice *Élaboration d'un plan de biosûreté exhaustif* à :

Courriel de l'ASPC : PHAC.standards.normes.ASPC@canada.ca

Courriel de l'ACIA : standardsnormes@inspection.gc.ca



ABRÉVIATIONS AND ACRONYMES



ABRÉVIATIONS ET ACRONYMES

ABCSE	Agent biologique à cote de sécurité élevée
ACIA	Agence canadienne d'inspection des aliments
ASB	Agent de la sécurité biologique
ASPC	Agence de la santé publique du Canada
ELR	Évaluation locale des risques
GCB	<i>Guide canadien sur la biosécurité</i>
GR	Groupe de risque (c.-à-d. GR1, GR2, GR3, GR4)
GRC	Gendarmerie royale du Canada
Habilitation de sécurité en vertu de la LAPHT	Habilitation de sécurité en vertu de la <i>Loi sur les agents pathogènes humains et les toxines</i>
LAPHT	<i>Loi sur les agents pathogènes humains et les toxines</i>
LSA	<i>Loi sur la santé des animaux</i>
NC	Niveau de confinement (c.-à-d. NC1, NC2, NC3, NC4)
NCB	<i>Norme canadienne sur la biosécurité</i>
PIU	Plan d'intervention d'urgence
PON	Procédure opératoire normalisée
RAPHT	<i>Règlement sur les agents pathogènes humains et les toxines</i>
RPV	Réseau privé virtuel
RSA	<i>Règlement sur la santé des animaux</i>
RTMD	<i>Règlement sur le transport des marchandises dangereuses</i>
SCRS	Service canadien du renseignement de sécurité
TI	Technologies de l'information
TVCF	Système de télévision en circuit fermé

INTRODUCTION



CHAPITRE 1 - INTRODUCTION

1.1 Portée

Toutes les **installations**, y compris les installations de niveau de confinement 2 (NC2), visées par la *Norme canadienne sur biosécurité* (NCB), 2^e édition (p. ex. les entreprises qui détiennent un **permis** en vertu de la *Loi sur les agents pathogènes humains et les toxines* (LAPHT) ou qui importent en vertu de la *Loi sur la santé des animaux* (LSA) et du *Règlement sur la santé des animaux* (RSA) sont tenues d'élaborer un plan de **biosûreté**^{1,2,3,4}. Un plan de biosûreté est exigé de toute installation réglementée (Matrice 4.1 de la NCB). Les organisations peuvent avoir un plan pour chaque campus, chaque site ou chaque **niveau de confinement**, ou un plan pour de multiples sites, licences et niveau de confinement.

Au Canada, les installations qui exercent des **activités réglementées** visant des **agents pathogènes** humains ou des **toxines** sont régies par la LAPHT et le *Règlement sur les agents pathogènes humains et les toxines* (RAPHT), à moins qu'elles respectent les critères d'exclusion énoncés dans la LAPHT⁵. Les installations qui ne sont pas exclues ou exemptées par la LAPHT ou le RAPHT doivent être titulaires d'un permis pour mener des activités réglementées visant des agents pathogènes humains ou des toxines. L'**importation** au Canada d'**agents zoopathogènes**, d'animaux infectés, de produits ou de sous-produits d'animaux ou d'autres organismes porteurs d'un agent zoopathogène ou d'une partie de celui-ci (c.-à-d. les toxines), et les activités comportant le matériel importé, sont régies par la LSA et le RSA et nécessitent un permis d'importation d'agents zoopathogènes ou une autorisation de **transfert**. Au Canada, les activités visant des agents pathogènes humains et des agents zoopathogènes, des toxines et autres **matières infectieuses** réglementées sont régies par l'Agence de la santé publique du Canada (ASPC) ou l'Agence canadienne d'inspection des aliments (ACIA), conformément à la LAPHT, le RAPHT, la LSA et le RSA.

La NCB décrit les exigences minimales auxquelles doivent satisfaire les **zones de confinement** situées dans des établissements réglementés en vertu de la LAPHT, du RAPHT, de la LSA et du RSA, le cas échéant. Le *Guide canadien sur la biosécurité* (GCB), 2^e édition, 2016, complémentaire à la NCB, fournit des renseignements de base et des directives sur les moyens de satisfaire aux exigences énoncées dans la NCB⁶. Le GCB fournit également des directives sur l'élaboration et la mise à jour d'un programme de biosécurité axé sur les **risques**.

Le plan de biosûreté est un élément clé du programme de biosécurité. La ligne directrice *Élaboration d'un plan de biosûreté exhaustif* renferme des précisions sur les lignes directrices sur la biosûreté fournies dans le GCB afin d'aider les installations à satisfaire aux exigences en matière de biosûreté énoncées dans la NCB.

1.2 Aperçu

La **manipulation ou l'entreposage** d'agents pathogènes humains, d'agents zoonopathogènes ou de toxines présentent un risque pour le personnel, la **communauté** et l'environnement. La gestion de ces risques nécessite une sensibilisation et l'application de pratiques relatives à la biosécurité et à la biosûreté de la part du personnel travaillant en **laboratoire** et dans d'autres zones de confinement où sont manipulés des agents pathogènes, des toxines, des matières infectieuses ou des animaux infectés.

Un programme de biosûreté vise à prévenir la perte, le vol, l'utilisation malveillante, le détournement ou la **libération** intentionnelle de **ressources biologiques** (c.-à-d. d'agents pathogènes, de toxines ou autres matières infectieuses réglementées), et de ressources liées d'une installation (p. ex. **matières biologiques** non infectieuses, matériel, animaux, renseignements de nature délicate). La présente ligne directrice porte sur l'élaboration d'un plan de biosûreté exhaustif qui repose sur une **évaluation des risques de biosûreté** liés aux ressources que possède une installation, ainsi qu'aux activités réalisées dans celle-ci. Toutes les installations doivent posséder un plan de biosûreté, mais sa complexité (p. ex. le niveau de détail, les mesures de sécurité) est proportionnelle au risque posé par la compromission des ressources que possède l'installation, déterminé au cours de l'évaluation des risques de biosûreté.

Le présent document fournit des orientations détaillées sur les éléments nécessaires à l'élaboration d'un plan de biosûreté dans les installations où des agents pathogènes et des toxines sont manipulés ou entreposés, afin de satisfaire aux exigences minimales en matière de biosûreté présentées dans la NCB, la LAPHT et le RAPHT, et de fournir des éléments de réflexion plus approfondis allant au-delà des orientations de base incluses dans le GCB. Cela comprend des orientations sur l'élaboration d'un plan de biosûreté exhaustif et la mise en œuvre de mesures de contrôle et de procédures en matière de biosûreté adaptées aux risques déterminés dans l'évaluation des risques de biosûreté.

1.3 Utilisation de la Ligne directrice canadienne sur la biosécurité : Élaboration d'un plan de biosûreté exhaustif

Les renseignements fournis dans la ligne directrice *Élaboration d'un plan de biosûreté exhaustif*, y compris les exemples présentés, visent seulement à fournir une orientation pour améliorer un plan de biosûreté. Ils ne doivent pas être interprétés comme des exigences. Certaines sections comprennent un tableau présentant un élément du plan de biosûreté, le risque qui doit être atténué et un exemple sur la façon dont ce risque peut être atténué dans le cas d'un NC2, d'un NC3, ou d'une zone où on manipule ou entrepose des **Agents biologiques à cote de sécurité élevée** (ABCSE). Ces exemples ont pour but de rappeler qu'un risque donné peut être commun à tous les niveaux de confinement, mais que la stratégie d'atténuation choisie est proportionnelle au risque identifié pour une zone ou une aire de **confinement** particulière. Aux endroits où les lignes directrices renvoient à une exigence de la NCB, la ou les matrices liées à cette exigence sont citées en référence (p. ex. matrice 4.1 de la NCB). De la même façon, aux endroits où les lignes directrices renvoient à une exigence provenant de la loi (c.-à-d. de la LAPHT, du RAPHT, de la LSA ou du RSA), l'article concerné, ainsi que le ou les paragraphes concernés, le cas échéant, seront cités en

référence (p. ex. LAPHT 33). Le présent document guidera l'utilisateur en déterminant les mesures de contrôle appropriées à mettre en œuvre, adaptées aux risques particuliers identifiés par l'évaluation des risques de biosûreté. Les exigences minimales pour l'élaboration d'un plan de biosûreté sont énoncées dans la matrice 4.1 de la NCB.

La ligne directrice *Élaboration d'un plan de biosûreté exhaustif* comprend une liste détaillée des abréviations et des acronymes utilisés dans ce document; cette liste se trouve au début du document. Chaque terme pour lequel il existe une abréviation ou un acronyme est écrit au long à sa première occurrence, l'abréviation suivant immédiatement entre parenthèses; seuls les abréviations et les acronymes sont utilisés pour le reste du document.

La présente ligne directrice comprend également un glossaire exhaustif où sont définis les termes techniques au chapitre 9; les termes qui y figurent sont inscrits en **caractères gras** à leur première occurrence. Le chapitre 10 fournit une liste des ressources qui ont servi à élaborer la Ligne directrice. Les citations dans le texte sont présentées dans les références à la fin de chaque chapitre. Des renseignements supplémentaires sur la biosécurité et la biosûreté se trouvent dans le GCB et sur le portail d'apprentissage en ligne de l'ASPC (santepublique.gc.ca/formation).

Références

1 Gouvernement du Canada. (2015). *Norme canadienne sur la biosécurité*, 2e éd., Ottawa, ON, Canada : Gouvernement du Canada.

2 *Loi sur les agents pathogènes humains et les toxines (L.C. 2009, ch. 24)*. (2015).

3 *Loi sur la santé des animaux (L.C. 1990, ch. 21)*. (2015).

4 *Règlement sur la santé des animaux (C.R.C., ch. 296)*. (2015).

5 *Règlement sur les agents pathogènes humains et les toxines (DORS/2015-44)*. (2015).

6 Gouvernement du Canada. (2016). *Guide canadien sur la biosécurité*, 2e éd., Ottawa, ON, Canada : Gouvernement du Canada.

POUR COMMENCER



CHAPITRE 2 - POUR COMMENCER

2.1 Rôles et responsabilités

La **haute direction** de l'installation est l'autorité responsable de la délégation des pouvoirs en matière de biosûreté. La personne à qui le rôle a été délégué peut être l'**agent de la sécurité biologique** (ASB) ou un autre représentant de la biosécurité, ou ce pourrait être le personnel de la sécurité ou une autre personne désignée; cependant, l'élaboration et la mise en œuvre réussies d'un plan de biosûreté exigent souvent la contribution d'une équipe d'experts en la matière possédant un vaste éventail de connaissances et de compétences, et une vaste expertise. Les membres de l'équipe peuvent comprendre un ou des gestionnaire(s), agent(s) des finances, architecte(s), une firme d'ingénieur, l'ASB ou le représentant de la biosécurité, le personnel de la sécurité, des scientifiques, des travailleurs de laboratoire, le personnel d'entretien et les autorités locales responsables de l'application de la loi, selon les situations particulières.

Les responsabilités de la personne déléguée consisteront à former une équipe (au besoin), à élaborer, à mettre en œuvre et à améliorer le plan de biosûreté; elle pourra agir à titre de personne-ressource pour tout **incident** de biosûreté, tenir à jour une liste des personnes qui ont accès à des agents pathogènes, à des toxines et à d'autres matières infectieuses réglementées, maintenir des registres de formation et s'assurer que des mesures sont en place afin de protéger de façon adéquate les renseignements de nature délicate. La NCB précise qu'il revient à l'ASB (ou au responsable de la biosécurité) de communiquer avec l'ASPC et l'ACIA au nom du titulaire du permis ou du détenteur du permis d'importation d'agents zoopathogènes^{1,2}.

D'autres personnes jouent des rôles essentiels dans le maintien de la biosûreté. Dresser la liste de ces personnes et leurs coordonnées dans le plan de biosûreté est essentiel à l'élaboration et à la mise en œuvre du plan. Ces personnes clés pourraient comprendre :

- les personnes désignées comme étant titulaires du Permis d'agent pathogène et de toxine, et les détenteurs d'un permis d'importation d'agents zoopathogènes;
- les personnes responsables de la gestion et de la supervision du programme ou du projet de **recherche scientifique** (p. ex. le chercheur principal, les gestionnaires ou le directeur du laboratoire/de l'installation);
- le responsable de la sécurité sur place (le cas échéant). Le plan de biosûreté devrait décrire ses responsabilités (p. ex. surveiller les systèmes de détection d'intrusion, intervenir en cas d'alarmes, tenir les registres des entrées/sorties des visiteurs, émettre des cartes d'identité), particulièrement en ce qui a trait à la biosûreté;
- les autorités locales responsables de l'application de la loi. Tout autre rôle joué par les autorités locales d'application de la loi pourrait être présenté dans un protocole d'entente (PE), le cas échéant;
- tout le personnel ayant accès à des agents pathogènes ou à des toxines qui comportent un risque plus élevé (p. ex. ABCSE, **groupe de risque 3** [GR3], GR4);
- les personnes chargées de l'examen de la fiabilité du personnel et de l'évaluation des résultats;

- les ressources humaines, qui peuvent participer à la gestion liée aux problèmes de comportement et faciliter les communications avec les programmes d'aide aux employés et les syndicats, le cas échéant;
- les personnes responsables des technologies de l'information (TI) et de la sécurité du réseau;
- toutes les personnes (personnel d'entretien, animaliers, personnel de la sécurité, etc.) qui peuvent prendre en charge à distance les **systèmes de contrôle d'accès** de l'intérieur ou de l'extérieur de l'installation (p. ex. par les systèmes de contrôle automatique du bâtiment, les ordinateurs ou les consoles de la sécurité).

2.2 Évaluation des risques de biosûreté

La NCB précise que l'élaboration d'un plan de biosûreté, propre à un lieu, doit être fondé sur l'évaluation des risques associés aux ressources (c.-à-d. agents pathogènes, toxines et autres ressources liées) que possède une installation, ainsi qu'aux activités réalisées dans celle-ci³. Le risque est fondé sur la probabilité qu'un événement se produise, et la gravité des conséquences de cet événement. L'évaluation des risques de biosûreté est une évaluation de la probabilité d'un événement *intentionnel*, comme le vol de ressources (p. ex. agent pathogène, toxine, matière infectieuse, équipement, animaux, renseignements), et les conséquences de cet événement (p. ex. incidence sur la santé publique résultant de la libération intentionnelle d'un agent pathogène, ou le vol d'information exclusive). Elle détermine et classe par ordre de priorité les risques qui seront atténués par les stratégies recommandées et les pratiques exemplaires décrites dans le plan de biosûreté.

L'évaluation des risques de biosûreté diffère de l'évaluation des risques de biosécurité (p. ex. évaluation globale des risques, évaluation des risques associés aux agents pathogènes et aux toxines, et **évaluation locale des risques** [ELR]), dans la mesure où des personnes ou des groupes qui peuvent montrer un intérêt malveillant à l'égard d'une ressource (p. ex. des menaces) doivent également être pris en considération lors de l'évaluation de la probabilité de survenue d'un événement. Les menaces peuvent être classées en deux groupes : les personnes ou les groupes sans accès autorisé aux ressources sont considérés comme des **menaces externes**, et les personnes et les groupes ayant un accès autorisé aux ressources, comme des **menaces internes**⁴.

De plus, l'évaluation des risques de biosûreté doit tenir compte des exigences accrues relatives à la sécurité des ressources avec une **possibilité de double usage**, c'est-à-dire celles qui peuvent être utilisées pour des applications scientifiques légitimes, mais qui présentent un risque de biosûreté accru en raison d'une possibilité intrinsèque d'élaboration et d'utilisation comme une arme biologique. Les ressources pouvant avoir un double usage comprennent les agents pathogènes et les toxines qui sont des ABCSE, mais elles peuvent inclure également des ressources liées à la manipulation et entreposage (p. ex. l'équipement et les renseignements)⁵. Les étapes pour mener une évaluation des risques de biosûreté sont décrites au chapitre 6 du GCB.

Les énoncés et les niveaux de risque déterminés par l'évaluation des risques de biosûreté peuvent être consignés de diverses façons (p. ex. registre sur les risques) et constituent le point de départ de l'élaboration de tout plan de biosûreté.

2.3 Élaboration du plan de biosûreté

Le plan de biosûreté expose en détail les stratégies d'atténuation relatives aux risques de biosûreté qui ont été identifiés, associés aux ressources biologiques. Le plan de biosûreté décrit les mesures de contrôle physique et opérationnel mises en œuvre afin de prévenir l'accès non autorisé aux ressources et de détecter les incidents où l'accès non autorisé a été tenté et d'intervenir.

Le plan de biosûreté devrait servir de complément aux mesures d'atténuation présentées dans le **Manuel de biosécurité**, le **plan d'intervention d'urgence** (PIU), les plans de sécurité pour un établissement et les programmes d'aide aux employés. Des contrôles d'accès peuvent déjà exister à certains niveaux dans ces plans ou documents (p. ex. certains risques de biosûreté sont peut-être déjà gérés par des mesures mises en œuvre pour traiter des risques de biosécurité). Par exemple, le processus de présélection du personnel et des mesures de sécurité physique peuvent être utilisées pour atténuer les risques de biosécurité et de biosûreté (matrice 4.1 de la NCB). L'intégration des éléments du plan de biosûreté dans l'ensemble du programme de biosécurité permettra une gestion plus efficace de la biosécurité et réduira les renseignements redondants.

2.3.1 Éléments d'un plan de biosûreté

Tous les plans de biosûreté doivent tenir compte des six éléments qui sont examinés dans le présent document. Ces éléments et leur objectif de rendement sont les suivants :

- **Sécurité physique** : réduire le risque d'accès non autorisé aux ressources et autres documents de nature délicate en adoptant des mesures de sécurité physique.
- **Compétence et fiabilité du personnel** : réduire le risque d'accès non autorisé à des ressources en évaluant la fiabilité actuelle et continue d'une personne à occuper un poste.
- **Responsabilités relatives aux agents pathogènes et aux toxines** : établir la « propriété » des agents pathogènes et des toxines, et préciser la responsabilité et l'autorité des personnes.
- **Gestion de l'inventaire** : empêcher les menaces internes en assurant un suivi des agents pathogènes, des toxines, des matières infectieuses et des ressources liées, et en permettant l'identification rapide des articles manquants.
- **Incident et intervention d'urgence** : promouvoir la sécurité et la sûreté des agents pathogènes et des toxines; fournir une base de données probantes visant l'amélioration continue des mesures de biosûreté.
- **Gestion de l'information et sécurité** : protéger les renseignements de nature délicate contre l'accès non autorisé ou le vol, et assurer le niveau de confidentialité requis.

2.3.2 Élaboration des mesures d'atténuation des risques

L'élaboration des mesures d'atténuation des risques de biosûreté devrait s'appuyer sur une approche systématique fondée sur des processus opérationnels bien documentés afin de cerner, d'évaluer et de communiquer les enjeux liés aux risques, et de prendre des décisions concernant ces derniers, dans un effort pour déterminer les meilleures mesures à prendre. Toutes les mesures pour protéger une ressource donnée devraient atteindre le même niveau de protection. Par exemple, l'entrée principale et les sorties de secours devraient être protégées au même niveau de protection et toutes les personnes (personnel et visiteurs) ayant accès à une zone de confinement devraient satisfaire aux mêmes conditions d'entrée.

Chaque organisation possède une culture du risque (p. ex. les attitudes et les comportements au sein d'une organisation concernant la gestion des risques) et une tolérance du risque (p. ex. la volonté d'une organisation d'accepter ou de rejeter un niveau de risque résiduel donné)⁶. La culture et la tolérance du risque peuvent changer en fonction des priorités organisationnelles, des intervenants et de la disponibilité des ressources. Elles doivent être bien comprises par l'équipe multidisciplinaire chargée de l'évaluation des risques de biosûreté et, ultérieurement, de l'élaboration des mesures d'atténuation qui seront exposées en détail dans le plan de biosûreté.

2.3.2.1 Mesures d'atténuation proportionnelles aux risques de biosûreté

Étant donné que le plan de biosûreté est fondé sur l'évaluation des risques de biosûreté, celui-ci sera adapté à chaque installation ou zone de confinement, et son niveau de détail et de complexité variera selon la nature (p. ex. la taille, la structure, la complexité) de l'installation et les activités réalisées dans chaque zone de confinement (p. ex. une installation de NC2 pour la réalisation de travaux *in vitro* présentera moins de risques de biosûreté aux fins de l'atténuation qu'une installation de NC3 pour la réalisation de travaux comportant des ABCSE).

Toutes les installations réglementées sont tenues d'élaborer un plan de biosûreté qui tient compte des six éléments décrits à la section 2.3.1, mais un bon nombre de mesures d'atténuation excèdent celles nécessaires à l'atténuation des risques dans de nombreuses installations de NC2. Lors de l'élaboration d'un plan de biosûreté pour une installation donnée, l'objectif de rendement de chaque élément du plan de biosûreté devrait être pris en considération en ce qui concerne les risques identifiés dans l'évaluation des risques de biosûreté. Ensuite, les mesures de contrôle qui seront appropriées pour gérer les risques identifiés seront soigneusement prises en considération.

Les chapitres qui suivent exposent plus en détail la théorie qui sous-tend chaque élément de la biosûreté et donnent des exemples de mesures de contrôle physique et opérationnel qui peuvent être utilisées pour atténuer les risques de biosûreté.

2.3.3 Accès au plan de biosûreté selon le besoin de connaître

Le plan de biosûreté complet et détaillé contient de l'information sensible, telle que des **vulnérabilités**, des risques, des mesures spécifiques d'atténuation des risques, des plans d'étage, des systèmes de sûreté et les détails de contrôle de l'accès. L'accès au plan de biosûreté complet et aux évaluations des risques de biosûreté détaillées, qui comprennent le registre des risques, devrait être limité aux **personnes autorisées** (p. ex. l'ASB, le personnel de sécurité, la haute direction, les inspecteurs de l'ASPC et l'ACIA désignés en vertu de la LAPHT ou de la LSA) avec le besoin de connaître pour l'exercice de leurs fonctions. Les renseignements détaillés que contient le plan ne sont pas destinés pour tout le personnel de l'installation. Le chapitre 7 fournit de plus amples renseignements sur la classification de l'information.

Le Manuel de biosécurité doit comprendre une description du plan de biosûreté (matrice 4.1 de la NCB). Cette description peut être un aperçu ou une version abrégée des mesures d'atténuation des risques de biosûreté qui s'appliquent à tout le personnel, tout en excluant les détails sensibles. Cette version peut être utilisée pour la formation du personnel et comprendrait les **procédures opératoires normalisées** (PON) propres à la biosûreté. Dans des circonstances où cela est jugé approprié, la formation peut cibler des groupes d'individus avec des fonctions semblables (p. ex. des travailleurs de laboratoire manipulant seulement des agents pathogènes de GR2, ou ceux qui manipulent des ABCSE).

Références

- 1 *Loi sur les agents pathogènes humains et les toxines* (L.C. 2009, ch. 24). (2015).
- 2 *Règlement sur les agents pathogènes humains et les toxines* (DORS/2015-44). (2015).
- 3 Gouvernement du Canada. (2015). *Norme canadienne sur la biosécurité*, 2e éd., Ottawa, ON, Canada : Gouvernement du Canada.
- 4 Salerno, R. M., & J. Gaudioso. (2007). *Laboratory Biosecurity Handbook*. Boca Raton, FL, États-Unis : CRC Press.
- 5 CEN Workshop 55 – CEN Workshop Agreement (CWA) 16393:2012, *Laboratory biorisk management – Guidelines for the implementation of CWA 15793:2008*. (2012). Bruxelles, Belgique : Comité Européen de Normalisation. Consulté le 9 février 2016 à l'adresse <http://www.valvira.fi/documents/14444/259268/CWA+16393/36d5eeb3-a206-4aec-a0b3-2bea97459835>.
- 6 Gouvernement du Canada (2012). *Guide de gestion intégrée du risque: Approche recommandée pour la préparation d'un profil de risque organisationnel*. Consulté le 9 février 2016 à l'adresse <http://www.tbs-sct.gc.ca/hgw-cgf/pol/rm-gr/girm-ggir/girm-ggirtb-fra.asp>

SÉCURITÉ PHYSIQUE



CHAPITRE 3 - SÉCURITÉ PHYSIQUE

La sécurité physique désigne les obstacles ou les mesures mises en place afin d'empêcher physiquement l'accès non autorisé à une installation, à une partie d'une installation, ou aux ressources, et de les protéger contre les dommages, le vol ou leur utilisation malveillante. La sécurité physique adéquate devrait être mise en œuvre afin de réduire les possibilités que des personnes non autorisées entrent dans les zones de confinement et autres aires (p. ex. les aires d'entreposage), et empêcher l'enlèvement non autorisé d'agents pathogènes, de toxines, d'autres matières infectieuses réglementées, ou d'autres ressources de l'installation.

La complexité du système de sécurité physique devrait être proportionnelle au niveau de risque associé aux ressources, déterminée par une évaluation des risques de biosûreté. On consultera la NCB pour les exigences en matière de **confinement** physique et les **exigences opérationnelles** particulières à chaque niveau de confinement¹.

L'aspect relatif à la sécurité physique du plan de biosûreté devrait déterminer et décrire les systèmes de sécurité en place qui limitent ou restreignent l'accès aux zones contenant des agents pathogènes, des toxines et autres ressources. Les systèmes de sécurité physique en place (p. ex. dispositifs inviolables, alarmes, système de télévision en circuit fermé [TVCF], éclairage), exécutent une ou plusieurs fonctions pour contrôler ou empêcher l'accès aux ressources, détecter les tentatives d'accès non autorisé et intervenir en cas d'incidents².

Les sections suivantes aideront à déterminer le niveau de sécurité physique approprié. Des éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté associés à la sécurité physique se trouvent dans le tableau 3-2.

3.1 Barrières physiques et protection graduelle

Les mesures visant à prévenir l'accès aux personnes non autorisées sont habituellement situées dans le périmètre du site. Certains exemples de mesures comprennent ce qui suit : clôture de périmètre, systèmes de contrôle d'accès électroniques, dispositifs de verrouillage, fenêtres et portes de haute sécurité.

La première étape pour déterminer les **barrières de sécurité** physique les plus appropriées consiste à répertorier tous les points d'accès dans la zone de confinement (p. ex. portes, fenêtres et autres voies de pénétration). Dans les établissements où des ABCSE sont présents et accessibles, on doit tenir compte du mécanisme visant à limiter l'accès à la partie de l'installation où des ABCSE sont manipulés et entreposés aux personnes autorisées possédant une **Habilitation de sécurité en vertu de la LAPHT** valide.

Les mesures de sécurité physique peuvent être mises en œuvre de façon graduelle afin d'offrir un plus grand degré de protection dans le cas des matières biologiques qui présentent un risque plus élevé (p. ex. les ABCSE). Pour ce faire, il faut créer des zones multiples, imbriquées, exigeant des personnes qu'elles traversent une barrière de contrôle d'accès à chaque zone pour atteindre davantage de zones sécurisées dans l'installation (figure 3-1).

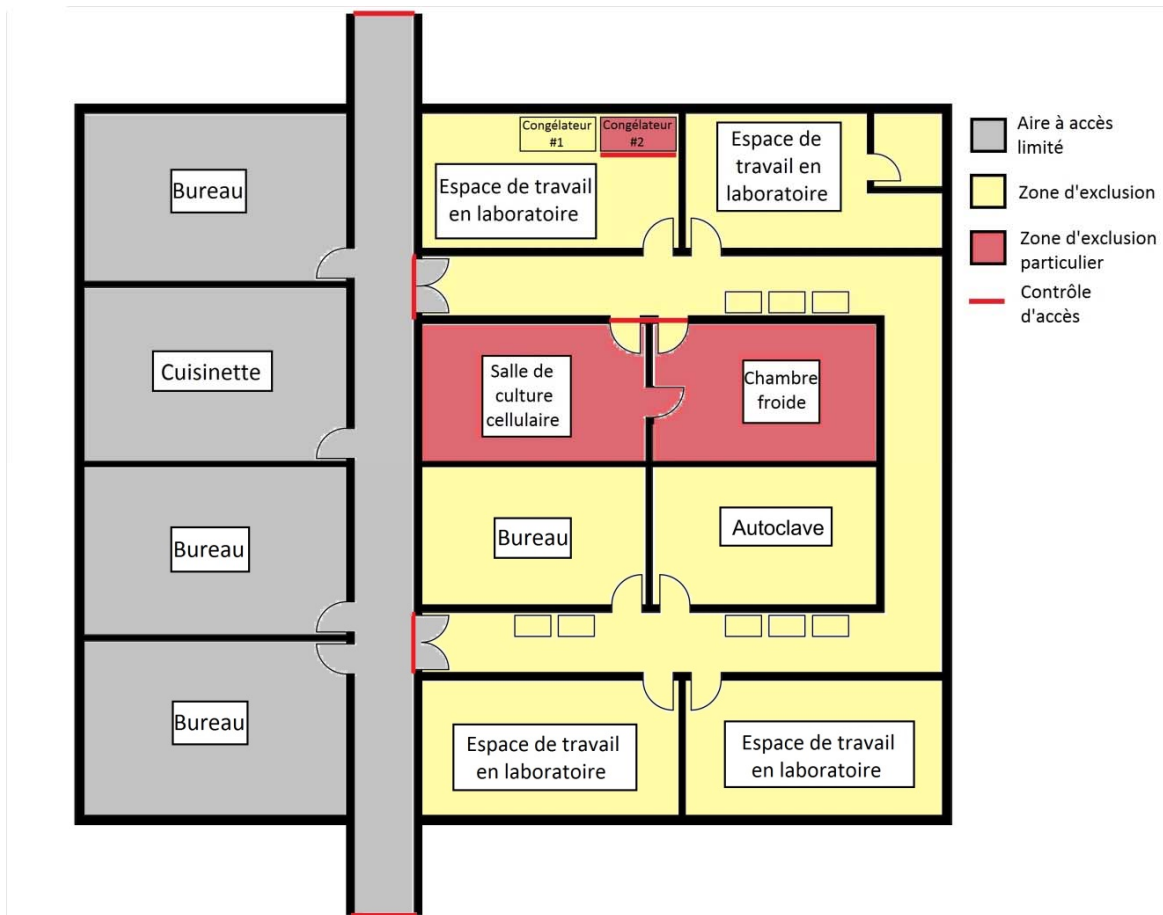


Figure 3-1 : Exemple de zones de protection graduelle dans une installation.

L'accès aux bureaux de l'installation et aux aires communes (cuisinette), indiqué en gris, est limité au personnel autorisé à accéder à l'installation. Des contrôles d'accès supplémentaires, indiqués par des lignes rouges aux points d'entrée, limitent l'accès à une aile des laboratoires (en jaune) au personnel de laboratoire autorisé. Un niveau supplémentaire de contrôles restreint l'accès à des aires particulières (en rouge) dans l'aile des laboratoires au personnel autorisé. Le contrôle d'accès au congélateur # 2 dans la salle de congélateur peut s'agir d'un cadenas de haute sécurité sur le congélateur.

3.1.1 Barrières de sécurité supplémentaires

Les barrières multiples peuvent également obliger les personnes non autorisées à utiliser différentes stratégies pour déjouer chaque barrière, ce qui retarde ces personnes et donne au personnel d'intervention le temps d'agir. Les barrières de sécurité supplémentaires comprennent les systèmes de verrouillage ou de restriction pour protéger l'équipement, et les coffres-forts et les congélateurs verrouillables pour l'entreposage des matières dans les espaces communs ou partagés. Par exemple, l'équipement d'entreposage verrouillé, fixé sur place, au mur ou au plancher, comme une armoire, un congélateur ou un réfrigérateur, de façon qu'il ne puisse être déplacé, est nécessaire si des ABCSE sont entreposés à l'extérieur de la zone de NC2 ou de NC3.

Un lieu d'entreposage ou un contenant sécuritaire devrait :

- être équipé d'un mécanisme de verrouillage robuste ou faire l'objet d'autres mesures afin de prévenir l'accès ou l'enlèvement non autorisé;
- faire en sorte que le contenu demeure protégé lorsqu'il est laissé sans surveillance;
- être équipé d'un système pour détecter l'entrée ou l'accès non autorisé.

3.1.2 Déterminer les aires où des ABCSE sont présents

La décision quant aux « locaux (ou parties) d'une installation dans lesquels sont autorisées des activités réglementées à l'égard d'ABCSE » sera prise par l'installation, en tenant compte de ce qui est le plus approprié à sa situation particulière. Il peut s'agir d'un simple local possédant les caractéristiques de sécurité uniques nécessaires aux ABCSE et un **accès limité** à un petit nombre de membres du personnel, ou une aire plus grande qui comprend plusieurs locaux ou l'ensemble du bâtiment qui respecte les mêmes exigences en matière de biosûreté, et qui est accessible à de nombreux membres du personnel.

Par exemple, à la figure 3-1, la partie de l'installation réservée aux ABCSE peut être définie comme étant :

- l'ensemble de l'aire représentée;
- l'aile des laboratoires, y compris la chambre froide et la salle de culture cellulaire;
- la salle de culture cellulaire, la chambre froide et le congélateur # 2.

Chaque scénario comportera des avantages et des inconvénients, comme le besoin de mesures de sécurité physique supplémentaires et de procédures opérationnelles de biosûreté; par exemple, le nombre de membres du personnel nécessitant une Habilitation de sécurité en vertu de la LAPHT valide, et les procédures opérationnelles qui devront être mises en place afin de donner l'accès aux membres du personnel sans habilitation de sécurité.

3.2 Mesures de contrôle d'accès

Les mesures de contrôle d'accès physique et opérationnel restreignent ou limitent au personnel autorisé l'entrée aux parties d'une installation où des agents pathogènes ou des toxines sont manipulés ou entreposés, ou bien où d'autres ressources de nature délicate sont présents. Le type de système de contrôle d'accès le plus approprié (p. ex. verrous à clés non reproductibles, lecteurs de cartes d'accès électroniques, claviers électroniques, systèmes à codes d'accès, lecteurs biométriques) dépendra de la situation particulière.

Les mesures suivantes sont des exemples de moyens utilisés pour contrôler l'accès aux ressources :

- o établir des points d'entrée « contrôlés »;
- o mettre en place des dispositifs de verrouillage activés manuellement, des cadenas, un lecteur de cartes d'accès ou des dispositifs/systèmes biométriques aux points d'entrée « contrôlés »;
- o mettre en place une alarme locale près des aires sécurisées pour avertir le personnel à proximité d'une intrusion ou d'un autre problème.

Des exemples de mesures de contrôle d'accès sont résumés au tableau 3-1. Les mesures de contrôle d'accès opérationnelles sont examinées à la section 3.4.

3.2.1 Fenêtres

Les fenêtres et autres ouvertures qui pourraient permettre l'accès à des endroits sécurisés, comme des conduits de ventilation, peuvent être munies de barres, d'une grille métallique ou de treillis en métal déployé pour assurer une sécurité accrue. Les pellicules plastiques de sécurité et de sûreté, et le vitrage de sécurité peuvent également aider à tenir ensemble les fragments de verre et à empêcher la fenêtre de sortir de son cadre en cas de bris. Sur le plan de la sécurité, les pellicules intimités peuvent être également d'une certaine utilité dans certaines situations (p. ex. des fenêtres dans des zones de confinement d'animaux). Cependant, ces pellicules offrent une intimité seulement dans certaines conditions d'éclairage. La quincaillerie de sécurité des fenêtres devrait être fixée de l'intérieur pour empêcher toute manipulation, ou être munie d'ancrages indémontables si elle est fixée à l'extérieur. Les fenêtres situées au rez-de-chaussée étant plus accessibles, il faut mettre en place des mesures supplémentaires (p. ex. de plus petites ouvertures) pour empêcher l'accès à celles-ci.

En ce qui concerne la résistance du verre, la plupart des types de verre peuvent être brisés à l'aide d'un objet dur (p. ex. une pierre). Cependant, le verre trempé et le verre laminé sont plus épais et plus résistants que le verre en feuille. Certains types de verre (p. ex. le verre laminé) résistent également à la fragmentation lorsqu'ils sont brisés.

Tableau3-1 : Aperçu des mesures de contrôle d'accès et des points à prendre en considération pour leur sélection et leur mise en place³

Mesure de contrôle d'accès	Pratiques en matière de sécurité et points à prendre en considération
Clé mécanique	- Utilisation de clés non reproductibles - Suivi de toutes les clés distribuées au personnel autorisé, consigné dans un registre qui est conservé et mis à jour - Changement de serrures ou de clés si une clé est perdue ou compromise - Retour immédiat des clés lorsque le personnel n'a plus besoin d'accès ou en cas de démission ou de cessation d'emploi - Protection de l'entreposage des clés non distribuées (p. ex. dans un coffret à clés)
Clé à code - serrure à combinaisons	- Conservation dans un dossier d'une liste des personnes avec des codes d'accès ou des clés - Changement des codes d'accès ou des serrures si les codes ou les clés sont compromis - Documentation de tous les changements aux codes d'accès, en considérant que ces renseignements sont de nature délicate - Conservation des registres des clés dans un registre et mise à jour - Conservation dans un dossier d'une liste des membres du personnel qui peuvent changer les codes
Cartes-clés électroniques	- Suivi de toutes les cartes-clés distribuées au personnel, consignées dans un registre ou une base de données - Conservation des registres des cartes-clés dans un registre et mise à jour - Photo d'identification, nom et date d'expiration sur les cartes-clés électroniques - Retour des cartes-clés au moment de la démission ou de la cessation d'emploi d'un membre du personnel - Programmation des cartes-clés afin de permettre l'accès aux aires à accès restreint, au besoin seulement (c.-à-d. l'accès à ces aires est annulé lorsqu'un membre du personnel n'a plus besoin d'y avoir accès)
Biométrie	- Conflit potentiel des systèmes biométriques avec les exigences liées à la biosécurité (p. ex. une lecture d'empreintes digitales serait inappropriée dans une aire où le personnel doit porter des gants) - Exigences relatives à la sécurité de l'information provenant des bases de données biométriques
Ouverture à distance (p. ex. appuyer sur un bouton-signal pour permettre l'entrée)	- Conservation dans un dossier de la liste des personnes ayant un accès autorisé - Élaboration et suivi des protocoles ou PON - Exigences relatives à la sécurité de l'information de ce système
Reconnaissance visuelle par un garde de sécurité	Garde de sécurité en poste aux points d'entrée pour vérifier visuellement les pièces d'identité
Types de mesures de contrôle d'accès multiples à une même porte	Utilisation de pratiques complémentaires en matière de sécurité (p. ex. carte-clé électronique et reconnaissance visuelle par un gardien de sécurité) pour assurer un niveau de sécurité accru

3.2.2 Portes

Les portes qui donnent accès à des aires où des ressources sont manipulées ou entreposées devraient être verrouillées lorsque les aires ne sont pas utilisées. Les portes à parement métallique ou les portes à âme pleine en bois installées dans un cadre renforcé fait d'un matériau de revêtement équivalent offriront un important niveau de protection. L'utilisation de charnières à gonds indémontables, dans le cas où celles-ci sont montées du côté exposé, contribuera à éviter que les portes soient enlevées. Lorsque des portes comprennent des fenêtres et des événements, la pose d'un vitrage de sécurité, de barres, d'une grille métallique ou de grilles équivalentes sur les grands événements empêchera qu'elles soient brisées ou enlevées. Les grilles devraient être fixées à l'aide d'ancres indémontables. Le GCB exige l'affichage d'un panneau d'avertissement de danger biologique sur les portes des zones de confinement pour éviter l'entrée non intentionnelle du personnel non autorisé. De même, la pose d'affiche sur d'autres portes, comme les portes de sortie de secours, peut aider à éviter l'entrée non intentionnelle (p. ex. une affiche indiquant « sortie de secours seulement »).

3.2.3 Clôtures et portes

Les installations qui abritent des ressources posant un risque élevé peuvent envisager l'installation d'une clôture autour du périmètre extérieur du bâtiment. Les clôtures de moins de 2.13 mètres de hauteur ne sont pas considérées comme étant des mesures de dissuasion efficaces.⁴ Le nombre de points d'entrée et de sortie dans la clôture devrait être limité le plus possible en gardant les barrières verrouillées lorsqu'elles ne sont pas utilisées, ou en installant, à chaque barrière, un poste de contrôle d'accès, occupé par du personnel de sécurité en tout temps. Munir le sommet de la clôture de fil barbelé ou d'un fil plat tranchant constitue des mesures de dissuasion supplémentaires.

3.2.4 Matériel de verrouillage

L'efficacité d'un matériel de verrouillage dépend de sa qualité de fabrication (p. ex. l'alignement des broches), de l'installation, de sa conception (le nombre de broches, les matériaux utilisés) et de son bon état. Il existe de nombreux types de serrures à clé qui diffèrent les uns des autres par le mécanisme (p. ex. serrures à gorge, à barillet, à levier). Les serrures sans clé, comme les serrures à combinaisons, utilisent un mécanisme à roulette. L'emploi de serrures à combinaisons ou de serrures sans clé avec code chiffré n'est pas recommandé pour protéger les ressources qui exigent un niveau élevé de sécurité. Les serrures à code munies d'un clavier numérique ou alphanumérique sont vulnérables aux personnes ou groupes qui sont capables de déduire le code d'accès à partir de l'apparence des clés. Aucune serrure n'offre une protection garantie, mais l'expertise et le temps nécessaires pour déjouer une serrure de haute sécurité par la force ou l'habileté peuvent suffire à dissuader les personnes non autorisées. Si des clés et des serrures classiques sont utilisées, elles devraient être de qualité élevée ou faire partie de serrures de haute qualité, comme les modèles à clés munis de barillet de haute sécurité comprenant un deuxième jeu de broches, à l'épreuve du crochetage ou de clés non reproductibles (p. ex. double taillé par des serruriers, des quincaillers ou pince coupante maison interdite). Dans le cas des cadenas, les modèles protégés en acier de haute sécurité peuvent être utilisés.

Les serrures portatives (p. ex. les cadenas à clé) peuvent être utilisées pour attacher plusieurs objets ensemble, généralement en utilisant une manille. Les serrures devraient être faites de matériaux durs résistant aux attaques utilisant la force et être munies de manilles blindées pour empêcher qu'elles soient coupées. Il n'est pas recommandé d'utiliser les cadenas à ressorts lorsqu'un niveau de sécurité raisonnable est nécessaire car il est possible de désengager le mécanisme de verrouillage en insérant une cale, et si le cadenas est endommagé ou perforé, le cadenas pourrait s'ouvrir soudainement.

Les passe-partout et les passe-partout partiels sont parfois utilisés dans les installations pour permettre aux personnes qui doivent accéder à de nombreuses salles de déverrouiller plusieurs portes à l'aide d'une seule clé. Dans une série de serrures à clé passe-partout partiel, une clé de groupe peut ouvrir toutes les serrures de la série et la clé maîtresse, un ensemble de serrures dans la série. Les systèmes de verrouillage équipés d'un passe-partout et d'un passe-partout partiel sont largement déconseillés, car la perte ou le vol d'une seule clé pourrait compromettre la sécurité d'une aire complète, et également parce que ces serrures sont généralement plus faciles à forcer (présence de plusieurs points de cisaillement dans l'alvéole).

Il existe deux types de corps de serrure sur les portes : les pènes demi-tour et les pènes dormants. Les pènes demi-tour ont une extrémité biseautée et sont à ressort, de sorte que la porte se verrouille automatiquement lorsqu'elle est fermée. Un des inconvénients du pêne demi-tour est qu'il est moins sécuritaire qu'un pêne dormant, sauf si le verrou est équipé d'un dispositif anti-cale; une porte verrouillée avec un seul verrou peut être ouverte assez facilement en utilisant une mince cale (p. ex. une carte de crédit). Un pêne dormant ne peut être déplacé qu'en position verrouillée ou ouverte à l'aide d'une clé (ou du bouton rotatif à partir de l'intérieur). Les pènes dormants qui dépassent le cadre de porte d'au moins 2.4 cm offrent une bonne protection.

3.2.5 Systèmes de contrôle d'accès électroniques

Les systèmes de contrôle d'accès électroniques, comme les systèmes biométriques et les lecteurs de cartes d'accès, peuvent être utilisés pour offrir un accès limité au personnel autorisé seulement. Les justificatifs d'identité sont présentés au système de contrôle d'accès à un point d'entrée. Une base de données branchée à un lecteur vérifie les renseignements de la personne, notamment si celle-ci est autorisée ou non à entrer à un point d'accès en particulier. La carte-clé peut comporter une bande magnétique qui est lue par le lecteur, ou comporter un élément qui est balayé par le lecteur lorsque la carte est tenue à proximité. Les systèmes de lecture de cartes sont les systèmes de contrôle d'accès électroniques les plus courants; la carte-clé est souvent utilisée comme carte d'identité. Un des avantages des systèmes de lecture de cartes est que les privilèges associés à la carte peuvent être facilement modifiés dans la base de données lorsqu'il y a un changement dans la situation d'emploi ou lorsqu'une carte-clé est perdue ou volée. Une autre source ou une source auxiliaire d'alimentation électrique de secours devrait être installée en cas de panne là où le système de contrôle d'accès est électronique. Si le système d'accès restreint retombe en mode fermeture en cas de panne, une solution de rechange serait de mettre en œuvre un système d'accès restreint de secours (p. ex. serrure à clé non reproductible).

Voici quelques-unes des caractéristiques générales des systèmes de contrôle d'accès électroniques :

- Capacité de déterminer et d'enregistrer où l'accès a eu lieu et les justificatifs d'identité utilisés
- Capacité de permettre ou d'interdire l'accès en fonction de l'heure du jour
- Capacité de changer l'autorisation d'accès sans apporter de modifications au matériel
- Capacité de surveiller la position d'une porte pour indiquer si elle est ouverte, fermée ou verrouillée
- Capacité d'apparier les renseignements sur les personnes (p. ex. photo, statut de l'employé, date d'expiration de l'accès)
- Capacité d'être reliés avec d'autres dispositifs de sécurité électroniques, comme des caméras

Une limite des systèmes électroniques de contrôle d'accès qui devrait être prise en considération est la possibilité d'interférences (p. ex. un enchevêtrement), soit par le système de contrôle automatique du bâtiment ou la console de sécurité sur les lieux, soit à partir d'un ordinateur ou d'un dispositif d'un endroit hors des lieux. Le **talonnage**, soit de permettre à quelqu'un d'entrer avec soi dans l'aire contrôlée, est une autre limite courante dans les lieux de travail, car il est considéré comme poli de tenir la porte ouverte à des collègues de travail. Une solution possible consiste pour la personne qui tient la porte ouverte de vérifier les cartes d'identité des collègues de travail. Les politiques organisationnelles et les attentes envers le personnel devraient être clairement décrites durant la formation de sensibilisation à la sécurité. La formation sur la sécurité est examinée plus en détail à la section 7.2.

Il existe de nombreux types de dispositifs biométriques qui peuvent être utilisés pour limiter l'accès à une installation ou à une partie de celle-ci. Les systèmes peuvent être axés sur la reconnaissance de l'iris, de la main, des empreintes digitales, de la voix ou du système vasculaire d'une personne. Un lecteur optique est utilisé pour saisir l'information de la personne. Cette information est comparée à une base de données contenant les éléments numérisés des personnes autorisées. Si une correspondance est identifiée, la personne se voit accorder l'accès. Les taux d'erreurs des systèmes biométriques peuvent varier selon la mesure dans laquelle les caractéristiques changent d'une journée à l'autre. Par exemple, un système de reconnaissance de la voix peut rejeter à tort une personne autorisée qui a un mal de gorge.

Tableau 3-2 : Éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté dans une zone de NC2, de NC3 et d'ABCSE

Élément du plan de biosûreté	Risque	Éventuelles mesures d'atténuation des risques		
		NC2	NC3	Zone d'ABCSE
Sécurité physique	Individu non autorisé accédant à la zone de confinement.	• Serrure à clé sur la porte menant à la zone de confinement. • Procédure qui interdit la reproduction de clés par les employés.	<u>Option A</u> • Serrure à clé non reproductible sur la porte menant à la zone de confinement. • Procédure pour la suppression de l'autorisation d'accéder à la zone. <u>Option B</u> • Accès à la zone par carte-clé électronique. • Système d'accès restreint de sauvegarde utilisant serrure à clé non reproductible. • Le contrôle d'accès retombe en mode fermeture en cas d'urgences.	<u>Option A</u> • Serrure à clé non reproductible sur la porte menant à la zone de confinement. • Procédure pour contrôler l'accès lorsqu'un individu ne détient pas une Habilitation de sécurité en vertu de la LAPHT valide. • Procédure pour la suppression de l'autorisation d'accéder à la zone. <u>Option B</u> • Accès à la zone par carte-clé électronique. • Système d'accès restreint de sauvegarde utilisant serrure à clé non reproductible. • Le contrôle d'accès retombe en mode fermeture en cas d'urgences.
	Individu non autorisé accédant à des agents pathogènes ou des toxines entreposés à l'extérieur de la zone de confinement.	• L'équipement d'entreposage situé à l'extérieur de la zone de confinement doit être verrouillé avec une serrure à clé (p ex. les congélateurs sont verrouillés).	• L'équipement d'entreposage de la zone de confinement doit être verrouillé avec une serrure à clé non reproductible et situé dans une aire à accès limité.	• L'équipement d'entreposage situé à l'extérieur de la zone de confinement doit être verrouillé avec une serrure à clé non reproductible et fixé sur place.

3.3 Détection des accès non autorisés et des tentatives d'accès

Les systèmes de détection dans une installation servent généralement à surveiller et à protéger une aire (p. ex. le périmètre de l'installation, les zones à accès restreint) plutôt qu'un objet. Dans le cas de certaines installations de NC2, il peut être suffisant de mettre en place des procédures opérationnelles pour obtenir des renseignements sur une personne non reconnue. Dans les aires à sécurité plus élevée, des moyens physiques de détection peuvent être justifiés pour surveiller (p. ex. par des caméras de sécurité, TVCF ou des alarmes) et enregistrer (p. ex. un enregistrement électronique des accès) les personnes qui entrent ou qui quittent les aires.

Les mesures suivantes peuvent permettre de détecter rapidement les accès non autorisés ou les tentatives d'accès :

- observation visuelle;
- évaluation des alarmes par vidéo;
- dispositifs de détection d'intrusion;
- relevés d'**inventaire** (s'ils sont vérifiés fréquemment);
- seaux et autres dispositifs d'indication d'altération.

Les aires qui ne sont pas physiquement occupées (p. ex. en dehors des heures de travail) peuvent être protégées par des systèmes de détection d'intrusion et des alarmes. Les divers types de systèmes de détection d'intrusion sont décrits dans le tableau 3-3. Les capteurs d'un système de détection d'intrusion sont souvent placés aux points d'intrusion possibles (p. ex. les fenêtres). Si le système de détection d'intrusion est déclenché, il est préférable qu'une équipe d'intervention (p. ex. le personnel de sécurité, les autorités d'application de la loi) soit alertée le plus tôt possible de façon à déclencher une intervention rapide. Si des claviers sont utilisés pour activer ou désactiver un système de détection d'intrusion, le dispositif et sa boîte de jonction électrique devraient être installés dans un endroit protégé afin de réduire les risques d'altération.

3.3.1 Systèmes de détection des intrusions

Afin de détecter un accès non autorisé, une tentative d'accès ou une altération, un système de détection des intrusions devrait :

- s'activer dès la détection d'un acte d'intrusion ou d'une altération;
- continuer à produire une alarme jusqu'à ce qu'elle soit reconnue par une personne autorisée;
- utiliser plus d'un capteur ou d'un type de capteur afin de fournir une fonction de redondance;
- inclure des zones de détection qui se chevauchent;
- utiliser des liens de communications supervisés spécialisés qui sont continuellement surveillés;

- être équipé d'une source d'alimentation auxiliaire de secours ou l'équivalent pour maintenir une capacité de détection en continu en cas de perte de l'alimentation électrique principale;
- avoir un taux faible de déclenchement intempestif ou de fausses alarmes avec une probabilité élevée de détection.

De plus, il faut tenir compte des recommandations suivantes lors de l'utilisation de systèmes d'alarme intérieurs :

- Les dispositifs de surveillance et les batteries de secours devraient être protégés contre toute manipulation par des personnes non autorisées (p. ex. panneau électronique ou boîte de jonction)
- Les zones d'alarme spécialisées peuvent être utilisées dans les aires d'entreposage (p. ex. distinctes des autres zones d'alarme, comme l'**espace de travail en laboratoire**)
- Une piste d'audit devrait être maintenue pour enregistrer la cause de toutes les alarmes
- Un effectif suffisant devrait être présent en tout temps au poste de surveillance des alarmes

Tableau3-3 : Résumé des systèmes de détection d'intrusion

Système de détection	Description	Utilisations possibles	Limites	Attentes
Détecteur de mouvement à infrarouges	Détecte un changement dans la température ambiante.	- À l'intérieur des aires d'accès restreint - Le long des entrées menant aux aires d'accès restreint - À travers les portes fermées menant aux aires d'accès restreint - Près de l'équipement d'entreposage contenant des agents pathogènes ou des toxines	- Aires comportant des articles ou de l'équipement qui dégage de la chaleur - Aires très grandes - Salles où sont hébergés des animaux	Il doit être installé dans des aires stratégiques de l'installation.
Interrupteur magnétique	Détecte un circuit interrompu (p. ex. une porte ou une fenêtre ouverte).	Fenêtres ou portes menant aux aires d'accès restreint	Aires comportant des fenêtres en verre ou des portes donnant un accès direct aux aires d'accès restreint	Il peut exiger également des détecteurs de verre brisé
Détecteur de verre brisé	Détecte les fréquences et les vibrations provenant du verre brisé.	Laboratoires comportant des fenêtres en verre donnant accès aux aires d'accès restreint	- Installations situées dans des régions où de fortes tempêtes sont fréquentes - Installations ne comportant pas de fenêtres en verre	Toutes les portes et les fenêtres doivent être équipées d'un détecteur.
Détecteur acoustique de mouvement	Détecte le mouvement en émettant des ondes sonores qui sont réfléchies par les objets.	- À l'intérieur des aires d'accès restreint - Le long des entrées menant aux aires d'accès restreint - Près des portes menant aux aires d'accès restreint - Près de l'équipement d'entreposage contenant des agents pathogènes ou des toxines	- Locaux et salles animalières - Salles contenant de l'équipement bruyant (p. ex. agitateurs, incubateurs) - Aires très grandes	Le système doit être installé dans des aires importantes précises.

Détecteur acoustique	Surveille les sons afin de déterminer le moment où une intrusion se produit et la nature de l'intrusion.	- À l'intérieur des aires d'accès restreint - Le long des entrées menant aux aires d'accès restreint	- Locaux et salles animalières - Salles où il y a un bruit de fond (p. ex. salles contenant de l'équipement bruyant) - Installation sans amortissement sonore extérieur	Les sons extérieurs doivent être suffisamment bloqués (p. ex. les sons provenant du laboratoire situé à proximité).
Surveillance visuelle	Images vidéo captées par une caméra et surveillées par le personnel de la sécurité. (p. ex. la TVCF).	Les caméras peuvent être installées aux points d'entrée et dans le périmètre de l'installation.	La qualité vidéo varie en fonction des conditions de visibilité (p. ex. degré de luminosité et pluie forte).	Les images doivent être constamment surveillées par le personnel de sécurité ou le signal vidéo doit être enregistré et intégré au système de détection des intrusions.

3.3.2 Surveillance par télévision en circuit fermé

Les systèmes de surveillance par télévision en circuit fermé (TVCF) permettent au personnel de la sécurité de voir à l'intérieur de nombreuses aires à partir d'un emplacement central. De nombreux systèmes peuvent également inclure l'audio. Les systèmes les plus simples comprennent une caméra, un moyen de transmission du signal vidéo provenant de la caméra vers un lieu de visualisation, et une personne qui surveille la transmission vidéo en direct ou la vidéo enregistrée. Les systèmes plus complexes peuvent comprendre plus de caméras et de détecteurs de mouvement vidéo, un commutateur-mélangeur pour passer d'une caméra à une autre ou un multiplexeur permettant de voir plusieurs transmissions vidéo simultanément, un annotateur pour enregistrer l'heure et la date de la vidéo, et des ordinateurs qui assument les fonctions de traitement de l'image (p. ex. la reconnaissance d'objets, les fonctions de recherche et de lecture). Les caméras peuvent être placées à des endroits stratégiques à l'intérieur et dans le périmètre de l'établissement (p. ex. aux points d'entrée et de sortie, aux détecteurs raccordés aux alarmes). La vidéo filmée par un système de TVCF peut être utilisée comme preuve dans les enquêtes d'incidents.

Grâce à la transition de la technologie analogique à la technologie d'imagerie numérique, diverses fonctions de calcul peuvent être intégrées dans le système de sécurité. Par exemple, des vidéos peuvent être visionnées pour rechercher des séquences d'images inhabituelles, comme la présence d'une personne, d'un objet ou d'un véhicule qui pourrait être d'importance. Les caméras peuvent également être contrôlées à distance. Les améliorations technologiques ont également amené l'utilisation de caméras couleur à haute résolution.

Le système de TVCF peut également jouer un rôle dans l'intervention d'urgence. Il peut permettre au personnel de la sécurité de voir les endroits et d'évaluer la situation. Si le système de TVCF est intégré à un système de détection, il peut être utilisé pour déterminer la

cause d'une alarme d'intrusion (p. ex. s'il est déclenché par un humain). Les dossiers électroniques peuvent être copiés sur d'autres supports (p. ex. DVD, clé USB) pour être conservés à long terme, s'ils devaient servir d'éléments de preuve.

3.3.3 Technologie d'inviolabilité

Des rubans, étiquettes et seaux d'inviolabilité peuvent être utilisés pour détecter visuellement l'accès non autorisé afin de protéger des ressources tels que des congélateurs, flacons, boîtes ou autres contenants d'agents pathogènes ou de toxines. Les dispositifs offerts sur le marché comprennent les flacons à bouchon avec levier, permettant l'ouverture par pression sans décapsuleur, et les contenants qui peuvent être protégés au moyen de mécanismes en plastique qui se détachent à l'ouverture.

3.3.4 Éclairage

L'éclairage extérieur d'une installation peut être utilisé pour accroître la sécurité des personnes autorisées qui entrent dans le bâtiment et qui en sortent. Il peut également servir à dissuader ou à détecter l'intrusion en améliorant la qualité de l'image vidéo provenant des caméras extérieures. Les différents types d'éclairage comprennent les lampes incandescentes, les lampes à décharge à haute intensité, les lampes fluorescentes et les diodes électroluminescentes (DEL). L'éclairage devrait être choisi en fonction de l'utilisation prévue. Par exemple, l'éclairage à détection de mouvement doit atteindre son niveau maximal rapidement, et l'éclairage servant à la surveillance vidéo des zones peut nécessiter la diffusion de lumière d'une couleur particulière pour capter les détails de l'image.

Certains experts font valoir que les conditions de faible éclairage sont pires que s'il n'y avait pas d'éclairage. Il faut tenir compte du fait qu'une lumière de forte intensité facilite la détection visuelle d'intrus, tandis que l'obscurité totale assure un excellent couvert, et il devient également difficile pour un intrus de déjouer une barrière. Cependant, des conditions de faible luminosité peuvent être suffisantes pour permettre à un intrus de manipuler une serrure, mais insuffisantes pour permettre la détection par une caméra.

3.4 Considérations d'ordre opérationnel liées au contrôle d'accès

Des mesures opérationnelles de contrôle d'accès peuvent être utilisées seules ou en combinaison avec des mesures physiques pour restreindre l'accès à une installation ou à une partie de celle-ci. Des politiques et procédures en place (p. ex. pour le contrôle des clés, des codes et des visiteurs) et la formation des membres du personnel afin qu'ils comprennent et suivent les procédures établies sont essentielles au maintien d'une installation protégée. Les politiques et les procédures devraient décrire l'autorité responsable de l'installation qui a le pouvoir d'approuver le processus d'autorisation du personnel, et qui peut identifier les individus qui peuvent autoriser le personnel à accéder un aire quelconque. Le processus d'autorisation peut comprendre une série d'approbations (p. ex. des ressources humaines, du service de sécurité de l'installation et des superviseurs) et que l'individu ait respecté toutes les exigences d'accès (p. ex. qualifications professionnelles appropriées, formation en biosécurité

et biosûreté complétées, et, le cas échéant, une Habilitation de sécurité en vertu de la LAPHT) avant d'être accordé le droit d'accès.

3.4.1 Identifier le personnel autorisé

Un processus ou une politique devraient être établis pour accorder, modifier ou retirer l'autorisation d'accès lorsque des personnes (p. ex. personnel travaillant dans la zone de confinement, stagiaires, visiteurs, personnel de gestion, étudiants, personnel d'entretien, personnel d'intervention d'urgence) ont besoin d'un accès temporaire ou n'ont plus besoin de l'accès, ou lorsqu'elles démissionnent ou sont congédiées. Le processus peut nécessiter la désactivation des cartes-clés, le retour des clés, des cartes-clés et des cartes d'identité, ou le changement des codes de clés. La politique devrait définir les critères auxquelles il faut satisfaire avant que l'accès soit accordé, ce qui peut comprendre l'autorisation médicale, les besoins en formation et l'Habilitation de sécurité en vertu de la LAPHT, ou l'accompagnement et la supervision.

La liste des personnes autorisées devrait être révisée régulièrement. La révision peut être plus fréquente dans les installations où :

- des ABCSE sont manipulés ou entreposés;
- un grand nombre de personnes ont un accès (p. ex. installations plus grandes);
- le roulement des personnes ayant un accès est fréquent (p. ex. établissement d'enseignement);
- le roulement des projets est fréquent (p. ex. études sur les animaux).

Il faut également envisager de limiter l'accès aux systèmes et logiciels de gestion de la sécurité pour empêcher les interférences non autorisées.

3.4.2 Établir des procédures de contrôle d'accès

Des PON ou des protocoles écrits devraient être établis afin d'aider le personnel à déterminer si une personne est autorisée ou non à accéder à une installation, y compris les mesures à prendre pour identifier, affronter, renvoyer et signaler les personnes non autorisées et suspectes. Des politiques et des procédures devraient être mises en place pour permettre l'accès à l'installation aux personnes chargées du nettoyage, de l'entretien et de la réparation (p ex., personnes accompagnées ou agents pathogènes mis sous clé et inaccessibles). Une politique sur le port d'une carte d'identité avec photo (toujours présentée dans l'installation et jamais portée à l'extérieur de celle-ci) aidera à identifier les personnes autorisées.

Lorsque des codes de clés ou des cartes sont utilisés dans les systèmes de contrôle d'accès électroniques une politique devrait être établie interdisant au personnel de partager les justificatifs d'identité (p. ex. partager la carte ou le code de quelqu'un d'autre, ou permettre le talonnage). Les cartes-clés utilisées conjointement avec un code de clé augmentent le niveau de sécurité.

Finalement, une PON devrait être établie pour signaler la perte, le vol ou l'accès compromis de clés, de cartes ou de codes, de sorte que des mesures correctives puissent être mises en œuvre en temps opportun.

3.4.2.1 Clés

Des registres sur les clés et les systèmes connexes (p. ex. cartes-clés, codes et serrures à combinaisons) devraient être tenus à jour afin de limiter ou de restreindre l'accès aux zones de confinement, aux matières infectieuses ou aux toxines. Ces registres devraient comprendre les éléments suivants :

- le nom des personnes à qui la clé, le code ou la combinaison a été remis;
- la date de remise ou de révocation.

L'organisation devrait se doter d'un processus permettant de retirer les clés aux personnes dont l'accès n'est plus requis, ou demander à celles-ci de retourner les clés, et de ranger les clés non distribuées de manière sécuritaire (p. ex. dans une armoire ou un coffre-fort verrouillé).

Une bonne pratique de contrôle des clés consiste à :

- limiter le nombre de personnes ayant des clés à celles qui ont besoin d'un accès;
- limiter le nombre de passe-partout aux membres de la direction et aux personnes qui ont besoin d'entrer dans toutes les aires (p. ex. les agents de la sécurité biologique [ASB]);
- effectuer une vérification régulière (p. ex. mensuelle, semestrielle ou annuelle) de l'inventaire des clés et des détenteurs de clés, en fonction du roulement du personnel afin de tenir compte de toutes les clés distribuées et non distribuées, et des clés déclarées perdues ou volées;
- établir des voies de communication entre les détenteurs de clés et le service des ressources humaines afin de faciliter la notification des changements relatifs au statut d'emploi des personnes;
- interdire au personnel de copier les clés;
- utiliser une clé brevetée non reproductible ou une rainure de clé unique pour empêcher la copie non autorisée des clés;
- s'assurer que les clés distribuées au personnel de la sécurité, comme les passe-partout, sont remises d'un quart de travail à l'autre et qu'elles demeurent dans l'installation;
- changer les codes d'accès définis en usine par défaut lorsqu'une serrure est installée, le cas échéant.

Une clé pour l'accès en cas d'urgence devrait être rangée dans un endroit sécuritaire (p. ex. dans une boîte à clés protégée). Si la clé est utilisée dans une situation d'urgence, son utilisation devrait être consignée dans le registre des clés et la personne responsable devrait en être informée (p. ex. l'ASB).

3.4.2.2 Cartes d'identité

Les cartes d'identité avec photo émises par une organisation ne sont pas reliées à un système de contrôle d'accès électronique. Cependant, les cartes-clés électroniques peuvent également servir de carte d'identité si le nom et la photo de la personne autorisée apparaissent sur la carte.

Les cartes d'identité devraient comprendre une photo de la personne autorisée aux fins de sécurité et de comparaison avec d'autres personnes, le nom de la personne et la date d'expiration de la carte. Les cartes d'identité peuvent utiliser des codes de couleurs afin d'indiquer l'autorisation à des aires d'accès restreint précises d'une installation. Ce système permet au personnel à l'intérieur d'une aire d'accès restreint de surveiller et de détecter les personnes non autorisées. Par exemple, un garde de sécurité peut permettre à une personne de franchir un point de contrôle à partir de la vérification de ses justificatifs d'identité (p. ex. une carte d'identité valide avec photo, l'identification de la photo et le nom de la personne figurant sur la liste des personnes autorisées). Selon le niveau de sécurité requis, l'identification visuelle par un garde de sécurité n'est pas nécessairement l'option d'accès contrôlé la plus appropriée dans le cas d'organisations comptant de nombreux employés (plus de 30 employés par quart de travail).

Pour qu'un système de cartes d'identité fonctionne, toutes les personnes autorisées devraient présenter en tout temps leur carte lorsqu'elles sont dans l'établissement, à l'exception des aires où ce n'est pas autorisé (p. ex. NC3, NC4). Le personnel devrait vérifier de façon régulière l'identité des autres personnes qu'elles croisent tout au long de la journée, et tout employé qui ne possède pas de carte d'identité devrait être accompagné à la sortie de l'aire d'accès restreint ou déclaré à l'autorité interne compétente.

Les cartes d'identité délivrées au personnel qui ont besoin d'entrer dans l'installation ou à une partie de celle-ci doivent être documentées de la même façon que les clés décrites ci-dessus. Les cartes d'identité doivent être rapidement retournées au responsable de leur émission lorsque l'accès n'est plus requis (p. ex. modification de tâches, retraite, congédiement). Les privilèges d'accès associés aux cartes-clés électroniques peuvent être facilement modifiés dans le système d'accès électronique.

Un système d'échange est une procédure de contrôle opérationnelle qui peut être utilisée pour réduire le risque associé à la falsification des cartes d'identité. Les employés se voient remettre deux cartes d'identité comportant des photographies identiques. Une sert simplement à identifier l'employé, tandis que l'autre est codée (p. ex. avec une bordure ou une couleur de fond différente) pour indiquer clairement les parties de l'installation auxquelles la personne a accès. L'employé échange la carte d'identité non codée pour la carte codée au début de son quart de travail. À la fin du quart de travail, l'employé retourne la carte d'identité codée en échange de la carte non codée.

3.4.2.3 Cartes-clés électroniques

Les cartes-clés électroniques, qu'elles soient génériques ou qu'elles servent de cartes d'identité, peuvent être utilisées pour donner un accès électronique (p. ex. par un lecteur de cartes à bande magnétique, par proximité ou à puce). Dans les zones à sécurité moins élevée,

la carte seule peut être suffisante. Pour accéder à des zones à sécurité plus élevée, l'utilisation d'un code de clé associé empêchera l'accès non autorisé des personnes qui trouvent ou volent une carte.

3.4.2.4 Accompagnement et supervision

Les protocoles d'entrée des personnes en formation, des visiteurs, des étudiants, du personnel d'entretien, du personnel d'intervention d'urgence et autres personnes qui ont besoin d'un accès temporaire sont des éléments importants dont il faut tenir compte lors de l'évaluation du contrôle d'accès. Cela peut comprendre l'enregistrement du nom de la personne et de la date d'entrée, l'émission d'une carte d'identité temporaire qui définit clairement le but de sa présence sur les lieux (p. ex. visiteur, technicien en réparation) et le nom de la personne qui l'accompagne, le cas échéant.

Les personnes autorisées à entrer dans une partie de l'installation à accès restreint doivent satisfaire aux exigences de la NCB, de la LAPHT et du RAPHT. Des exigences organisationnelles supplémentaires déterminées par une ELR peuvent également s'appliquer.

Les procédures permettant aux visiteurs d'entrer dans les aires de l'installation où l'accès est limité ou restreint au personnel autorisé devraient être incluses dans le plan de biosûreté. Selon la zone de confinement, cela peut comprendre divers niveaux de supervision. Par exemple, un seul superviseur peut suffire pour un groupe d'étudiants universitaires visitant un laboratoire de NC2.

Dans le cas des installations où des ABCSE sont manipulés ou sont accessibles de toute autre manière, les personnes autorisées doivent posséder une Habilitation de sécurité en vertu de la LAPHT. L'accès est autorisé à une personne sans habilitation de sécurité (y compris les visiteurs) seulement lorsque des ABCSE sont mis sous clé et inaccessibles, ou lorsque la personne est accompagnée et supervisée de façon appropriée par une personne autorisée possédant une Habilitation de sécurité en vertu de la LAPHT. Cette dernière peut seulement accompagner et superviser une personne à la fois (RAPHT 23) et surveiller les activités de cette dernière en tout temps. Elle doit demeurer à l'affût de tout comportement douteux de la personne qu'elle accompagne.

Une personne qui s'est déjà vu refuser une Habilitation de sécurité en vertu de la LAPHT ou dont l'habilitation de sécurité a été suspendue ou révoquée n'est pas autorisée à entrer dans l'aire, même sous surveillance, à moins qu'une Habilitation de sécurité en vertu de la LAPHT ait été délivrée depuis le refus, la suspension ou la révocation (RAPHT 24).

3.4.2.5 Suppression de l'autorisation d'accès

Lorsqu'une personne n'a plus besoin d'accéder à une aire ou que son autorisation d'accès à une aire est révoquée, l'autorité responsable de l'installation devrait prendre les mesures pour supprimer l'autorisation aux aires dont l'accès n'est plus nécessaire. Dans les zones où des ABCSE sont manipulées ou entreposées, la suppression de l'autorisation d'accès doit s'effectuer immédiatement. Les mesures appropriées peuvent comprendre la récupération des

clés et de la carte d'identité, le changement des serrures et la mise à jour des registres d'accès électronique.

Dans les zones d'ABCSE, l'autorité responsable devrait immédiatement informer la personne concernée qu'elle n'a plus accès à la partie de l'installation, ou à l'installation tout entière. De plus, en vertu de la LAPHT et du RAPHT, l'ASPC doit immédiatement être avisée dans un tel cas (LAPHT 32, RAPHT 7). Les avis peuvent être transmis électroniquement à l'ASPC par le portail de la biosûreté accessible sur son site Web (www.publichealth.gc.ca/pathogens), par téléphone, par courriel (PHAC.LINC-DILC.ASPC@canada.ca) ou par télécopieur.

3.4.3 Sécurité et espaces communs

Un espace de laboratoire partagé est un modèle qui devient de plus en plus courant. Il s'agit d'un modèle de conception de laboratoires où il est possible de créer des environnements adaptés aux besoins actuels et pouvant satisfaire aux exigences futures. Les espaces partagés à l'intérieur des locaux d'un établissement où des activités réglementées menées avec des ABCSE sont autorisées en vertu d'un permis peuvent présenter des défis pour tout le personnel qui doit y pénétrer. Le service de gestion des installations, les directeurs et le détenteur du permis doivent déterminer la meilleure façon de faire face à ces défis.

Une solution possible consiste pour toutes les personnes qui travaillent dans des espaces partagés à se procurer une Habilitation de sécurité en vertu de la LAPHT, de façon à ce qu'elles puissent en tout temps entrer librement dans la partie de l'installation où des ABCSE sont présents. Ou encore, l'accès aux installations partagées par des personnes ne possédant pas une habilitation de sécurité (p. ex. celles pour lesquelles il n'est pas nécessaire d'avoir accès à des ABCSE) peut être limité aux moments où il n'y a pas d'ABCSE présents ou lorsque des ABCSE sont mis sous clés et sont inaccessibles, ou lorsque ces personnes sont accompagnées et supervisées par une personne qui possède une Habilitation de sécurité en vertu de la LAPHT pour cette partie de l'installation. Cette solution de rechange peut être appliquée par l'utilisation de calendriers et d'aires d'entreposage sécuritaires pour les ABCSE.

En ce qui concerne le partage d'un espace de laboratoire, les éléments suivants devraient être pris en considération :

- le type d'activité réalisée dans l'espace partagé;
- les personnes qui devront y avoir accès;
- la possibilité de séparer les activités par durée (heures particulières auxquelles des activités exigeant des mesures de sécurité accrues seront réalisées);
- les procédures relatives à la gestion des déchets d'ABCSE;
- le besoin de serrures et d'alarme sur de l'équipement précis, comme les congélateurs et les incubateurs qui contiennent des ressources, et pour les renseignements ou les aires d'entreposage des ressources.

Références

- 1 Gouvernement du Canada. (2015). *Norme canadienne sur la biosécurité*, 2e éd., Ottawa, ON, Canada : Gouvernement du Canada.
- 2 Fennelly, L. (2013). *Effective Physical Security* (4th ed.). Waltham, MA, États-Unis : Elsevier Inc.
- 3 Centers for Disease Control and Prevention (CDC) des États-Unis, Division of Select Agents and Toxins et Animal and Plant Health Inspection Service (APHIS) Agriculture Select Agent Program. (2013). *Security Guidance for Select Agent or Toxin Facilities* (2nd Revision). Consulté le 9 février 2016 à l'adresse http://www.selectagents.gov/resources/Security_Guidance_v3-English.pdf
- 4 United States Geological Survey, Department of Interior. des États-Unis. (2005). *Physical Security Handbook*, 440-2-H. Consulté le 15 mars 2016 à l'adresse <http://www.usgs.gov/usgs-manual/handbook/hb/440-2-h/440-2-h.html>

COMPÉTENCE ET FIABILITÉ DU PERSONNEL



CHAPITRE 4 - COMPÉTENCE ET FIABILITÉ DU PERSONNEL

Des politiques et des procédures devraient préciser et décrire les exigences relatives à la formation, à l'expérience, à la compétence et à la fiabilité du personnel ayant accès à des agents pathogènes, à des toxines ou à d'autres matières infectieuses réglementées. Des protocoles de vérification préalable à l'affectation devraient être élaborés afin d'évaluer l'intégrité des personnes qui auront accès à des agents pathogènes, à des toxines ou à d'autres matières infectieuses réglementées. Ces protocoles pourraient prévoir des références et des Habilitations de sécurité en vertu de la LAPHT. Des indicateurs de comportement devraient également être évalués à cette occasion. Un programme de fiabilité continue visant à promouvoir un comportement acceptable peut aussi être bénéfique en réduisant les risques associés au personnel. Par exemple, la disponibilité de programmes d'aide aux employés (p. ex. des services de consultation psychologique) est une méthode qui permet de réduire les risques qu'un employé qui éprouve des problèmes d'ordre personnel devienne une menace interne. Des éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté associés à la compétence et à la fiabilité du personnel se trouvent dans le tableau 4-1.

4.1 Vérification de la compétence et de la fiabilité

Des politiques et des procédures sur la collecte et la vérification des renseignements provenant des candidats, et la description de la façon dont ces renseignements seront évalués et utilisés pour déterminer la fiabilité d'un candidat, devraient être établies pour gérer le risque lié à une menace interne potentielle. Les exigences relatives à la formation, à l'expérience, à la compétence et autres exigences de fiabilité du personnel ayant accès à des agents pathogènes ou à des toxines devraient être clairement précisées et décrites. Il est également prudent de donner un aperçu des procédures relatives à l'évaluation de la fiabilité du personnel dans le plan de biosûreté. La rigueur du processus d'examen préalable (p. ex. le nombre d'années de données historiques examinées, le nombre de personnes données en référence qui ont été jointes, le nombre de sujets examinés) devrait être appropriée au niveau de risque associé aux ressources.

Par le truchement du processus d'embauche, les candidats qui font l'objet d'une enquête confirment qu'ils ont les qualifications, les compétences et les qualités personnelles appropriées pour entreprendre des travaux avec des agents pathogènes ou des toxines, et qu'ils sont les personnes les mieux qualifiées pour un poste avant de se voir offrir celui-ci et accorder l'accès à des agents pathogènes, des toxines ou d'autres ressources. Les attestations d'études, les antécédents professionnels, l'expérience de travail et l'historique de publication (p. ex. les renseignements contenus dans un curriculum vitæ) qualifient la capacité scientifique d'une personne, tandis que les références personnelles et professionnelles peuvent fournir une indication de la fiabilité d'une personne à manipuler des agents pathogènes et des toxines, ou à y avoir accès.

En plus des points mentionnés ci-dessus, les protocoles de vérification préalables à l'affectation peuvent comprendre les vérifications suivantes :

- immigration et statut du visa;
- antécédents criminels;
- autres critères jugés pertinents par l'établissement (p. ex. vérification du crédit, évaluation de la santé professionnelle, dépistage de drogues).

Si l'organisation qui s'occupe de l'embauche n'a pas accès aux outils nécessaires pour mener ces processus d'évaluation, les organismes locaux d'application de la loi peuvent être en mesure d'offrir de l'aide.

Tableau4-1 : Éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté associés à la compétence et à la fiabilité du personnel dans une zone de NC2, de NC3 et d'ACBSE.

Élément du plan de biosûreté	Risque	Éventuelles mesures d'atténuation des risques		
		NC2	NC3	Zone d'ABCSE
Compétence et fiabilité du personnel	Un individu qui ne répond pas aux exigences minimales de compétence et de fiabilité est accordé l'accès à des agents pathogènes et des toxines.	• La politique de préembauche comprend la vérification du curriculum vitæ du candidat, des références et de la preuve d'attestation d'études. • Les compétences comportementales et techniques du candidat sont évaluées par les références professionnelles.	• La politique de préembauche comprend la vérification du curriculum vitæ du candidat, des références, de la preuve d'attestation d'études et d'autres critères jugés pertinents (p. ex. la vérification de crédit). • Les compétences comportementales et techniques du candidat sont évaluées par les références professionnelles.	• La politique de préembauche comprend la vérification du curriculum vitæ du candidat, des références, de la preuve d'attestation d'études et d'une Habilitation de sécurité en vertu de la LAPHT valide. • Les compétences comportementales et techniques du candidat sont évaluées par les références professionnelles.

	Un individu qui ne répond plus aux exigences minimales de fiabilité continu d'avoir accès à des agents pathogènes et des toxines.	Programme d'évaluation continue de la fiabilité : • Procédure d'auto-déclaration et de déclaration par les pairs • Des mesures ou des sanctions disciplinaires progressives sont établies pour les individus qui ne se conforment pas aux pratiques établies de biosûreté. • Des procédures pour enlever ou supprimer temporairement l'accès d'un individu à des agents pathogènes et à des toxines ou à la zone de confinement.	Programme d'évaluation continue de la fiabilité : • Procédure d'auto-déclaration et de déclaration par les pairs • Des mesures ou des sanctions disciplinaires progressives sont établies pour les individus qui ne se conforment pas aux pratiques établies de biosûreté. • Des procédures pour enlever ou supprimer temporairement l'accès d'un individu à des agents pathogènes et à des toxines ou à la zone de confinement. • Une politique exigeant l'évaluation d'un individu au retour d'un congé pertinent (p. ex. congés pour cause de stress).	Programme d'évaluation continue de la fiabilité : • Procédure d'auto-déclaration et de déclaration par les pairs • Des mesures ou des sanctions disciplinaires progressives sont établies pour les individus qui ne se conforment pas aux pratiques établies de biosûreté. • Des procédures pour enlever ou supprimer temporairement l'accès d'un individu à des agents pathogènes et à des toxines ou à la zone de confinement. • Une politique exigeant l'évaluation d'un individu au retour d'un congé pertinent (p. ex. congés pour cause de stress). • Des procédures pour la déclaration de renseignements concernant toute circonstance à risque d'exercer une influence sur la validité de l'Habilitation de sécurité en vertu de la LAPHT de l'individu.
--	---	---	---	--

4.2 Programme d'évaluation de la fiabilité continue

Un programme de fiabilité continue vise à vérifier si une personne autorisée à accéder à des aires où sont présents des agents pathogènes, des toxines et d'autres ressources satisfait toujours aux critères de fiabilité du personnel, et à renforcer le comportement acceptable. Ce type de programme peut s'avérer bénéfique pour réduire les risques associés au personnel (p. ex. une menace interne) en offrant de l'aide aux employés qui éprouvent des problèmes. Il est important qu'une organisation demeure active et vérifie régulièrement les renseignements actuels pour s'assurer de la fiabilité continue de l'employé ayant accès à des agents pathogènes et à des toxines.

Le personnel devrait être encouragé de signaler aux autorités internes et au personnel de la sécurité tous renseignements qui peuvent avoir une incidence sur la sûreté ou la sécurité des individus, des ressources de l'installation ou de la collectivité dans son ensemble. Ces renseignements peuvent comprendre ce qui suit¹ :

- tout changement qui pourrait avoir une incidence sur l'Habilitation de sécurité en vertu de la LAPHT d'une personne;
- toute circonstance qui peut avoir une incidence sur la capacité d'une personne à effectuer ses tâches de manière sûre et sécuritaire (p. ex. augmentation du niveau de distraction ou d'erreurs; tendance accrue à prendre des risques);
- changements importants de comportement, d'attitude ou de manière d'agir, par exemple :
 - retrait des autres de plus en plus marqué;
 - détérioration importante et prolongée de l'apparence;
 - colère ou agressivité injustifiée;
 - signe de problèmes de toxicomanie (alcool ou drogues);
 - activité criminelle;
 - absences non expliquées.
- menaces implicites ou explicites proférées à l'égard des collègues, de l'organisme, de la sécurité des ressources, du bien-être des animaux de laboratoire ou du grand public;
- cas de non-conformité délibérée aux politiques institutionnelles et aux PON, ainsi qu'aux lois applicables et à la NCB;
- renseignements qui portent à croire que la personne n'est pas apte à réaliser son travail de manière sûre et sécuritaire;

- circonstances qui semblent douteuses, par exemple :
 - travaux de laboratoire qui ne correspondent pas au projet ou aux objectifs officiels;
 - demandes injustifiées de renseignements au sujet de la sécurité ou du laboratoire;
 - actes de vandalisme ou dommages matériels;
 - tentatives de faire entrer des amis ou des collègues dans des aires à accès restreints;
- Activités non autorisées réalisées par une personne en dehors des heures de travail.

Les organisations devraient envisager d'interdire ou de révoquer l'accès à une personne qui affiche des caractéristiques ou des comportements qui laissent croire qu'elle est incapable de travailler de façon sécuritaire ou d'assurer la sécurité des agents pathogènes, des toxines ou d'autres ressources manipulées ou entreposées dans l'établissement. Les organisations devraient établir des politiques relatives aux déclarations volontaires et aux déclarations par les pairs, et des protocoles de révocation d'une autorisation d'accès à une partie de l'installation ou aux ressources, ou de révocation immédiate d'une personne qui est réputée poser un risque inacceptable pour la sécurité. Toutes les personnes devraient être clairement informées de l'ensemble des politiques et des protocoles. Dans certains cas, les méthodes de rapports anonymes peuvent encourager le signalement des infractions et devraient être prises en considération lors de l'établissement des politiques et des procédures. Ces processus et ces procédures devraient être établis en consultation avec le service des ressources humaines de l'établissement.

4.3 Habilitation de sécurité en vertu de la LAPHT

Les risques accrus en matière de biosûreté associés aux ABCSE nécessitent des mesures de biosécurité supplémentaires, comme un contrôle de sécurité pour le personnel ayant accès à des ABCSE, afin d'atténuer les risques potentiels de menaces internes. Ainsi, le processus d'enquête de sécurité comprend une exigence supplémentaire pour les personnes travaillant dans une partie d'un établissement où des ABCSE sont manipulés ou autrement accessibles; ces personnes doivent obtenir une Habilitation de sécurité en vertu de la LAPHT, conformément à l'article 33 de la LAPHT². Le processus d'Habilitation de sécurité en vertu de la LAPHT est mené par la Gendarmerie royale du Canada (GRC) et le Service canadien du renseignement de sécurité (SCRS) au nom de l'ASPC, et il constitue un élément clé de la biosûreté du cadre réglementaire de la LAPHT visant à vérifier la crédibilité et la fiabilité de toutes les personnes ayant accès aux ABCSE. La figure 4-1 décrit les situations où l'Habilitation de sécurité en vertu de LAPHT est requise et non requise.

La section 6.3.3 du GCB fournit des renseignements supplémentaires sur la période de validité et la transférabilité des Habilitations de sécurité en vertu de la LAPHT. Ces renseignements concernant la suspension et la révocation d'une habilitation de sécurité et l'obligation d'aviser l'ASPC d'une infraction criminelle sont présentés aux sections 6.3.4 et 6.3.5, respectivement, du GCB³.

Accès à une partie de l'installation où des activités réglementées réalisées avec des ABCSE sont autorisées et sont en cours	Oui
Accès aux aires d'entreposage des ABCSE	Oui
Ouverture d'un coli contenant des ABCSE	Oui
Accès à une partie de l'installation où des activités réglementées réalisées avec des ABCSE sont autorisées lorsque des ABCSE sont mis sous clé et inaccessibles, ou enlevés complètement	Non
Accès à la partie d'une installation où des ABCSE sont présents et accessibles, pendant une supervision, selon un ratio de 1:1 par un détenteur d'une Habilitation de sécurité en vertu de la LAPHT valide	Non
Activité comportant l'utilisation de toxines constituant des ABCSE dont la quantité est inférieure à la limite établie	Non
Activité comportant l'utilisation d'un agent pathogène humain d'un groupe de risque donné qui a été atténué dans la mesure où il ne présente plus le profil de risque de ce groupe de risque.	Non
Transport (expédition) d'ABCSE à un autre endroit, de son emballage jusqu'à son ouverture par son destinataire	Non
Relève de la LTMD	

Figure 4-1 : Situations où une Habilitation de sécurité en vertu de la LAPHT délivrée par l'ASPC est exigée.

La *Loi sur le transport des marchandises dangereuses* (LTMD) régit les marchandises dangereuses en transit⁴.

Références

- 1 National Institutes of Health (NIH) des États-Unis, National Science Advisory Board for Biosecurity. (2011). *Guidance for Enhancing Personnel Reliability and Strengthening the Culture of Responsibility*. Consulté le 8 février 2016 à l'adresse http://osp.od.nih.gov/sites/default/files/resources/CRWG_Report_final.pdf
- 2 *Loi sur les agents pathogènes humains et les toxines* (L.C. 2009, ch. 24). (2015).
- 3 Gouvernement du Canada. (2016). *Guide canadien sur la biosécurité*. Ottawa, ON, Canada : Gouvernement of Canada.
- 4 *Loi de 1992 sur le transport des marchandises dangereuses* (1992, ch. 34). (2015).

RESPONSABILITÉ À L'ÉGARD DES AGENTS
PATHOGÈNES ET DES TOXINES, ET GESTION DE
L'INVENTAIRE



CHAPITRE 5 - RESPONSABILITÉ À L'ÉGARD DES AGENTS PATHOGÈNES ET DES TOXINES, ET GESTION DE L'INVENTAIRE

Les procédures relatives à la responsabilité à l'égard des agents pathogènes et des toxines, et à la gestion de l'inventaire sont établies dans le but de suivre et de consigner tous les agents pathogènes, les toxines et autres matières infectieuses réglementées **entreposés à long terme** au sein de l'organisation, et de protéger ces ressources contre la perte, le vol, l'utilisation malveillante, le détournement et la libération. Les mesures de contrôle des matières comprennent également les procédures visant à rendre compte du **déplacement** sécuritaire d'un agent pathogène ou d'une toxine dans l'organisation, ou de son **transport** dans un autre bâtiment de l'organisation, ou dans une organisation différente. Le niveau de responsabilité et les mesures de contrôle sont déterminés par l'évaluation des risques de biosûreté.

5.1 Responsabilité à l'égard des agents pathogènes et des toxines

La responsabilisation est un moyen d'établir la propriété des agents pathogènes et des toxines, et de définir les responsabilités de chaque personne autorisée à l'égard de la supervision des agents pathogènes et des toxines présents dans l'installation. En vertu de la LAPHT, du RAPHT, de la LSA et du RSA, toutes les personnes autorisées doivent rendre compte de leurs actions et de leurs décisions concernant les agents pathogènes, les toxines et autres matières infectieuses réglementées^{1,2,3,4}. Ces personnes doivent également rendre compte à leur superviseur, aux gestionnaires de la zone de confinement ou de l'installation, au détenteur de permis ou au détenteur de permis d'importation d'agents zoopathogènes, et peut-être aussi à l'ACSP et l'ACIA.

Dans le cas des agents pathogènes et des toxines à risque plus élevé (p. ex. des ABCSE, des agents de GR3 et de GR4), les mesures de responsabilisation devraient inclure des vérifications régulières de l'inventaire afin de confirmer l'exactitude de celui-ci et, le cas échéant, de s'assurer que les matières inventoriées ou l'inventaire en soi n'a pas été altéré. Cela peut se faire par une vérification matérielle afin de confirmer la présence des matières figurant dans l'inventaire, une vérification durant le déplacement ou le transfert de matières sur les lieux, d'une observation à distance par le système de TVCF, ou par une vérification des seaux ou des dispositifs d'invulnérabilité sur les contenants et l'équipement d'entreposage. Un processus de gestion de l'inventaire robuste peut comprendre une analyse périodique pour confirmer les contenus des contenants⁵. La tenue des registres d'entrée et de sortie de toutes les personnes confirme qui étaient présents dans la zone de confinement à tout moment. Ces renseignements peuvent être utilisés dans les enquêtes sur les agents pathogènes ou les toxines absentes de l'inventaire.

Des éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté associés à la responsabilité à l'égard des agents pathogènes et des toxines se trouvent dans le tableau 5-1. Une orientation supplémentaire sur la responsabilisation à l'égard des agents pathogènes et des toxines est fournie au chapitre 19 du GCB.

Tableau5-1 : Éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté associés à la responsabilisation à l'égard d'agents pathogènes et de toxines dans une zone de NC2, de NC3 et d'ABCSE.

Élément du plan de biosûreté	Risque	Éventuelles mesures d'atténuation des risques		
		NC2	NC3	Zone d'ABCSE
Responsabilisation à l'égard des agents pathogènes et des toxines	Un envoi d'agents pathogènes ou de toxines est perdue durant le transport.	• Une procédure exigeant le suivi de colis durant leur expédition. • Une procédure décrivant la structure hiérarchique et les délais pour les agents pathogènes et les toxines perdus durant le transport. • Une procédure pour informer l'ASPC d'un agent pathogène ou d'une toxine manquant.	• Une procédure exigeant le suivi de colis durant leur expédition. • Une procédure décrivant la structure hiérarchique et les délais pour les agents pathogènes et les toxines perdus durant le transport. • Une procédure exigeant que l'expéditeur confirme que la matière a été reçu par le destinataire.	• Une procédure exigeant le suivi de colis durant leur expédition. • Une procédure décrivant la structure de déclaration pour un ABCSE qui n'est pas reçu dans les 24 heures le temps de livraison prévu, ce qui comprend la notification obligatoire de l'ASPC. • Une procédure exigeant que l'expéditeur confirme que la matière a été reçu par le destinataire.

5.2 Inventaires et gestion de l'inventaire

Un inventaire des agents pathogènes, des toxines et autres matières infectieuses réglementées, entreposés à long terme (plus de 30 jours) dans la zone de confinement, est exigé selon la matrice 4.10 de la NCB; il constitue un élément important du plan de biosûreté. Cette exigence ne s'applique pas aux matières utilisées pendant moins de 30 jours (p. ex. une culture continue de matières infectieuses, des études à long terme d'animaux infectés). Les exigences relatives à l'inventaire et le niveau de détail des renseignements dans l'inventaire

seront proportionnels au risque associé aux matières entreposées et autres exigences de la zone de confinement ou de l'installation (p. ex. la conformité avec les normes de gestion de la qualité, telles que l'Organisation internationale de normalisation [ISO] 9001⁶). L'inventaire peut se présenter sous différents formats (p. ex. un registre écrit, une base de données électronique ou une feuille de calcul), pourvu qu'il reflète avec précision la présence des agents pathogènes et des toxines entreposés à long terme dans l'installation.

Dans le cas d'agents pathogènes et de toxines du GR2 entreposés à long terme, il suffit de consigner l'emplacement et le groupe de risque. Dans le cas d'agents pathogènes et de toxines du GR3, du GR4 et d'ABCSE entreposés à long terme, l'inventaire doit comprendre la mention précise des agents pathogènes et des toxines, ainsi qu'un moyen de repérer un échantillon manquant ou volé en temps opportun (p. ex. un bâtiment, une salle, l'emplacement exact dans un congélateur, le nombre de flacons).

Même s'il n'est pas obligatoire de tenir un inventaire des agents pathogènes et des toxines entreposés durant moins de trente jours, comme les matières récemment reçues ou celles en utilisation continue (p. ex. les cultures), la tenue d'un registre de toutes les matières entrant ou sortant de la zone de confinement constitue une bonne pratique. Même les notes ou les registres de laboratoire concernant les activités de diagnostic (p. ex. les cultures) peuvent être utiles en cas de disparition d'agents pathogènes ou de toxines.

Il est recommandé que les établissements passent en revue leur inventaire et leurs registres d'accès afin de vérifier l'exactitude de l'inventaire à la suite d'une activité ou d'un incident suspect au cours duquel on aurait pu y avoir accès.

Des mesures efficaces relatives à l'inventaire des agents pathogènes et des toxines entreposés à long terme peuvent être une bonne façon d'empêcher et de détecter les menaces internes. Les éléments à prendre considération pour la mise en œuvre d'un inventaire robuste des agents pathogènes et des toxines, et d'un système de responsabilisation sont les suivants :

- identification d'une personne qualifiée comme seule responsable de la tenue de l'inventaire;
- mise à jour de l'inventaire au fur et à mesure que des matières sont ajoutées ou enlevées;
- consignation de tous les transferts, de l'inactivation et de l'élimination des matières;
- consignation dans l'inventaire de tous les agents pathogènes, de toutes les toxines et autres matières infectieuses réglementées, y compris les matières entreposées à l'extérieur de la zone de confinement;
- détermination et consignation de toutes les personnes qui ont accès aux matières ou à la zone où les matières sont manipulées ou entreposées;
- renvois aux documents pertinents (p. ex. autorisation de transfert d'un agent zoopathogène, permis d'importation);
- étiquetage approprié de tous les agents pathogènes, de toutes les toxines et autres matières infectieuses réglementées, entreposés à long terme;
- étiquetage des articles en ordre séquentiel (p. ex. un flacon hors séquence peut être facilement détecté).

Le niveau de sécurité de l'information associé à l'inventaire devrait être corrélé avec le groupe de risque des agents pathogènes ou les toxines (p. ex. un agent pathogène de GR2 par opposition à ABCSE) et, à tout le moins, satisfaire aux exigences énoncées dans la NCB. Des éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté associés à la gestion de l'inventaire se trouvent dans le tableau 5-2. De plus amples renseignements sur la sécurité de l'information sont présentés au chapitre 7.

Tableau 5-2 : Éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté associés à la gestion de l'inventaire dans une zone de NC2, de NC3 et d'ABCSE.

Élément du plan de biosûreté	Risque	Éventuelles mesures d'atténuation des risques.		
		NC2	NC3	Zone d'ABCSE
Gestion de l'inventaire	Un agent pathogène ou une toxine manquant n'est pas détecté.	• Procédure exigeant la vérification semestrielle de l'inventaire par le gestionnaire de laboratoire et par l'ASB autant que nécessaire.	• Procédure exigeant la vérification semestrielle de l'inventaire par l'ASB et vérification trimestrielle par le gestionnaire de laboratoire.	• Procédure exigeant la vérification semestrielle de l'inventaire par l'ASB et vérification trimestrielle par le gestionnaire de laboratoire, avec augmentation de la taille de l'échantillon.

5.3 Sécurité durant le déplacement et le transport

Le plan de biosûreté devrait comprendre des politiques et des procédures décrivant les mesures de responsabilisation visant à protéger les agents pathogènes et les toxines contre les menaces internes et externes lorsque des matières sont déplacées ou transportées d'un endroit à un autre, ce qui comprend l'expédition d'agents pathogènes et de toxines à une autre installation, ainsi que leur déplacement d'un endroit à un autre dans le même bâtiment.

Des contrôles procéduraux peuvent également être établis afin de réduire le risque de biosûreté associé aux colis reçus, ce qui comprend la formation du personnel et l'établissement de protocoles pour les expéditions imprévues d'agents pathogènes ou de toxines. Tous les colis et articles devraient être inspectés avant qu'ils ne soient apportés dans une partie de l'installation autorisée à réaliser des activités réglementées ou enlevés de celle-ci.

Dans certaines installations, on peut avoir une aire de réception centralisée à partir de laquelle tous les colis sont emportés intacts (non ouvert) au destinataire par le personnel de l'installation. Par contre, d'autres installations pourraient désigner une « aire de réception d'échantillons » où tous les colis contenant des agents pathogènes, des toxines, ou toute autre matière infectieuse sont ouverts, la réception du coli documenté, et les échantillons triés pour le déplacement (ou le transport) à l'individu ou l'aire pour des manipulations ultérieures ou l'entreposage. Si l'aire de réception d'échantillons reçoit des ABCSE (c.-à-d. que le coli contenant des ABCSE est ouvert), cette aire de réception est considérée comme une partie de l'installation où des ABCSE sont manipulés ou entreposés et l'accès à cette aire doit être restreint aux seules personnes autorisées détenant une Habilitation de sécurité en vertu de la LAPHT valide lorsque des ABCSE sont présents et accessibles.

Tous les transferts entre les détenteurs d'un permis, qu'ils soient internes ou externes, devraient être signifiés à l'ASB avant le transfert, même dans des situations où la déclaration à l'ASPC ou à l'ACIA n'est pas requise.

5.3.1 Transferts internes

Les installations qui transfèrent des agents pathogènes ou des toxines dans l'organisation devraient inclure dans le plan de biosûreté les politiques et les procédures décrivant la façon dont les transferts auront lieu, y compris les dispositions relatives à la protection des agents pathogènes et des toxines contre le vol, la perte ou la libération (p. ex. une politique contre l'acte de laissés des agents pathogènes et des toxines sans surveillance dans des aires publiques).

Les installations qui transfèrent un **agent zoopathogène** importé au titre d'un permis d'importation d'agents zoopathogènes délivré par l'ACIA doivent obtenir l'autorisation de cette dernière pour procéder au transfert à un autre endroit que celui spécifié sur le permis d'importation, que ce transfert s'effectue à l'intérieur de l'installation ou entre des installations. Si le transfert constitue une activité autorisée au titre d'un Permis d'agent pathogène et de toxine délivré par l'ASPC, les transferts d'agents pathogènes humains et d'agents zoopathogènes sont autorisés et n'ont pas à être déclarés à l'ASPC.

Une entente de transfert d'une matière ou un enregistrement semblable peut être utilisé pour définir qui a le contrôle de la matière et qui en est responsable à chaque point dans le déplacement ou le transfert¹. Ces documents protègent contre les agents pathogènes et les toxines laissés sans surveillance, et peuvent prouver que toutes les personnes qui étaient en possession du colis possédaient la formation appropriée pour manipuler la matière. Dans le cas de matières à risque plus élevé, telles que les ABCSE, une signature ou un relevé de chaîne de possession fournira un registre de toutes les personnes qui en avaient la possession durant le transfert et confirmera qu'elles avaient l'Habilitation de sécurité en vertu de la LAPHT appropriée.

5.3.2 Transferts externes et exportations

En vertu de la LAPHT, toute personne qui transfère des agents pathogènes ou des toxines au Canada doit prendre les précautions nécessaires pour s'assurer que le destinataire détient un permis pour utiliser l'agent ou qu'il est exempté de l'obligation de détenir un permis. De façon similaire, l'expéditeur qui exporte des agents pathogènes humains et des toxines à l'extérieur du Canada doit prendre les précautions nécessaires pour s'assurer que le destinataire respectera les normes et les politiques de biosécurité et de biosûreté en vigueur dans le pays de destination. Il en va de même des agents zoopathogènes importés en vertu d'un Permis d'agent pathogène et de toxine délivré par l'ACSP. Les transferts d'agents zoopathogènes, ce qui comprend les agents pathogènes zoonotiques, importés en vertu d'un permis d'importation d'agents zoopathogènes délivré par l'ACIA ne peuvent s'effectuer qu'après avoir obtenu l'autorisation de l'ACIA.

La *Loi sur le transport des marchandises dangereuses* et son règlement d'application (LTMD, RTMD) s'appliquent aux expéditions de matières infectieuses et de toxines, de l'envoi à la réception^{7,8}. Bien qu'il existe des limites quant à la surveillance que l'organisation peut fournir une fois que les agents pathogènes et les toxines sont en transit, des mesures peuvent être prises avant l'envoi afin d'atténuer les risques de biosûreté, par exemple en choisissant un service de messagerie fiable pour transporter la matière, ou en ayant recours au personnel de l'installation autorisée, certifié en TMD.

L'ASB doit être avisé avant que des mesures soient prises pour importer ou recevoir un agent pathogène humain ou une toxine (LAPHT 4[1]). Cela permet de repérer le colis si celui-ci n'a pas été reçu dans un délai raisonnable après la date de livraison prévue. L'expéditeur et le destinataire peuvent être en mesure de suivre le colis à l'aide de l'outil en ligne du service de messagerie, le cas échéant. De plus, les ASB des deux établissements doivent être informés du transfert avant de prévoir les plans d'expédition. En vertu de la LAPHT, l'ASB doit également être avisé de toute expédition d'ABCSE qui n'a pas été reçue dans les 24 heures après la date et le temps de livraison prévus. Ensuite, l'ASB doit aviser l'ACSP par l'entremise du portail sur la biosûreté, accessible sur le site Web de l'ACSP (www.publichealth.gc.ca/pathogens), par courriel (PHAC.LINC-DILC.ASPC@canada.ca) ou par télécopieur.

Références

1 *Loi sur les agents pathogènes humains et les toxines* (L.C. 2009, ch. 24). (2015).

2 *Règlement sur les agents pathogènes humains et les toxines* (DORS/2015-44). (2015).

3 *Loi sur la santé des animaux* (L.C. 1990, ch. 21). (2015).

4 *Règlement sur la santé des animaux* (C.R.C., ch. 296). (2015).

5 Salerno, R. M., & J. Gaudioso. (2007). *Laboratory Biosecurity Handbook*. Boca Raton, FL, États-Unis : CRC Press.

6 *ISO 9001:2008, Systèmes de management de la qualité - Exigences*. (2008). Genève, Suisse: Organisation internationale de normalisation.

7 *Loi de 1992 sur le transport des marchandises dangereuses* (L.C. 1992, ch. 34). (2015).

8 *Règlement sur le transport des marchandises dangereuses*. (DORS/2001-286). (2015).

INTERVENTION EN CAS D'INCIDENT ET D'URGENCE



CHAPITRE 6 - INTERVENTION EN CAS D'INCIDENT ET D'URGENCE

Un incident est un événement qui peut causer du mal au personnel, à la communauté ou à l'environnement. Le PIU devrait comprendre des procédures pour réagir de façon rapide et efficace aux situations qui pourraient avoir des répercussions sur la biosûreté de la zone de confinement, ce qui peut inclure des événements tels que la libération intentionnelle ou non d'agents pathogènes ou de toxines, les catastrophes naturelles, la violence en milieu de travail, les menaces à la bombe, les infractions à la sécurité (p. ex. entrée non autorisée, accès non autorisé à des renseignements de nature délicate) et les situations d'urgence (p. ex. incendie, urgences médicales). Des éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté associés aux interventions en cas d'urgence se trouvent dans le tableau 6-2. L'intervention en cas d'urgence est examinée au chapitre 17 du GCB, et de plus amples renseignements sur la déclaration des incidents et les enquêtes sur les incidents sont présentés au chapitre 8 du GCB¹.

6.1 Déclaration des incidents

Les procédures établies pour déclarer les incidents devraient être conformes à la réglementation en vigueur, ainsi qu'aux procédures internes de déclaration et d'enquête de l'organisation. Les PON relatives à la déclaration des incidents et aux enquêtes sur les incidents font partie intégrante du PIU et devraient être élaborées afin de compléter les programmes existants à l'échelle de l'installation (p. ex. le programme de santé et de sécurité au travail) ou s'aligner sur eux.

C'est une exigence de la NCB que les incidents mettant en cause des agents pathogènes, des toxines ou d'autres matières infectieuses réglementées, des animaux infectés ou une défaillance des **systèmes de confinement** ou des systèmes de contrôle doivent être immédiatement signalés à l'autorité interne appropriée et, dans certains cas, à l'ASPC (matrice 4.9 de la NCB)². Par exemple, l'ASPC doit être avisé s'il y a des motifs de croire qu'un agent pathogène ou une toxine a été volée ou a autrement disparue.

Plus particulièrement, les incidents suivants relatifs à la biosûreté devraient être déclarés immédiatement au personnel ou à l'autorité appropriée de l'établissement :

- la perte ou la compromission de clés, de mots de passe, de combinaisons de sécurité, d'équipement d'accès à distance (p. ex. ordinateurs portatifs, ordinateurs de table et tablettes) ou d'autres renseignements de sécurité essentiels;
- l'accès non autorisé ou les tentatives d'accès à des aires restreintes, comme les zones qui possèdent des ABCSE, les zones de NC3 ou de NC4, ou les aires où sont présents des renseignements de nature délicate;
- toute personne ou toute activité suspecte;
- tout équipement manquant présentant un risque de double usage;
- les écarts dans l'inventaire ou des indications que l'inventaire a été altéré ou autrement compromis.

L'installation devrait déterminer et consigner les situations pour lesquelles la participation précoce du service de sécurité de l'établissement ou des autorités locales responsables de l'application de la loi peut être nécessaire.

6.2 Planification des interventions en cas d'incident

Des mesures coordonnées et efficaces en temps opportun à des situations précises qui sont graves et inattendues peuvent exiger une intervention immédiate et planifiée afin de réduire les effets nocifs sur le personnel, la communauté et l'environnement. Ainsi, les plans d'intervention en cas d'incident de biosûreté, particulièrement adaptés à l'organisation, à l'installation et à la zone de confinement, peuvent être inclus dans le PIU. Le tableau 6-1 énumère les cinq éléments pour assurer le succès d'un plan d'intervention en cas d'incident.

Tableau 6-1 : Cinq éléments clés pour assurer le succès d'un plan d'intervention en cas d'incident

1. Le plan met l'accent sur la protection de la vie humaine avant celle des biens.
2. Le personnel est formé pour réagir rapidement et efficacement à l'incident.
3. Le plan est le résultat de la collaboration entre le personnel de l'installation et les premiers intervenants.
4. Les premiers intervenants participent à la formation sur la préparation aux incidents.
5. Le plan traite des dangers immédiats et des effets secondaires sur les personnes qui travaillent dans l'établissement.

Selon la nature de l'incident, les interventions peuvent comprendre ce qui suit : évacuer ou confiner le secteur touché; aviser les premiers intervenants, comme les services d'application de la loi ou les services d'urgence; évaluer la gravité de l'incident (p. ex. perte du confinement, **exposition** ou libération possible); prévenir les incidents secondaires; déterminer et préserver la chaîne de preuves. Chaque incident devrait être documenté, y compris les fausses alarmes. Bien qu'un PIU soit inclus dans le Manuel de biosécurité, les aspects relatifs à la biosûreté doivent être décrits dans l'élément du plan de biosûreté touchant l'intervention en cas d'incident et d'intervention d'urgence, ou dans une référence au PIU incluse dans le plan.

Tableau 6-2 :: Éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté associés aux interventions en cas d'incidents et d'urgences dans une zone de NC2, de NC3 et d'ABCSE.

Élément du plan de biosûreté	Risque	Éventuelles mesures d'atténuation des risques.		
		NC2	NC3	Zone d'ABCSE
Interventions en cas d'incidents et d'urgences	Agent pathogène volé n'est pas déclaré.	• Procédure exigeant que le personnel mène une enquête sur tout agent pathogène ou toxine manquant. • L'ASB doit être informé si l'agent pathogène ou la toxine n'est pas retrouvé dans un délai raisonnable. • L'ASB doit informer l'ASPC ou l'ACIA de l'agent pathogène ou de la toxine manquant.	• Procédure exigeant d'informer immédiatement l'ASB. • L'ASB doit informer l'ASPC ou l'ACIA de l'agent pathogène ou de la toxine manquant sans délai. • L'ASB doit enquêter sur tout agent pathogène ou toxine manquant et conserver les éléments de preuve.	• Procédure exigeant d'informer immédiatement l'ASB. • L'ASB doit informer l'ASPC ou l'ACIA de l'agent pathogène ou de la toxine manquant sans délai. • L'ASB doit enquêter sur tout agent pathogène ou toxine manquant et conserver les éléments de preuve. • L'ASB doit déclarer aux organismes locaux d'application de la loi tous les cas présumés de vol.

	Une clé ou une carte d'accès à la zone de confinement perdue ou volée n'est pas déclaré.	• Procédure exigeant la déclaration du superviseur de laboratoire dans un délai raisonnable de toutes clés perdues ou volées. • La serrure est remplacée ou les cylindres reclés dans un délai raisonnable.	• Procédure exigeant la déclaration immédiate au superviseur et au service de sécurité de toutes clés perdues ou volées. • La serrure est remplacée ou les cylindres reclés sans délai. • La carte d'accès perdue ou volée est désactivée dès que c'est déclaré.	• Procédure exigeant la déclaration immédiate au superviseur, à l'ASB et au service de sécurité de toutes clés perdues ou volées. • La serrure est remplacée ou les cylindres reclés sans délai. • Des mesures de sécurité alternatives sont mises en œuvre temporairement jusqu'à ce que la serrure est remplacée ou les cylindres reclés (p. ex. les ABCSE sont relocalisés à un autre endroit sûr ou placés dans un équipement d'entreposage cadenassé). • La carte d'accès perdue ou volée est désactivée dès que c'est déclaré.
--	---	--	--	---

6.3 Enquête sur les incidents

Les incidents de biosécurité peuvent indiquer des lacunes dans les systèmes de biosûreté ou être attribuables à une erreur humaine. L'enquête et le rapport sur les incidents sont nécessaires pour permettre aux installations de définir précisément la situation, de déterminer la raison pour laquelle un incident s'est produit (p. ex., déterminer la ou les causes fondamentales), s'il s'agit d'un incident intentionnel ou d'un **accident**, et d'un événement isolé, et pour prendre des mesures correctives pour éviter que des incidents similaires se produisent.

À la suite d'un incident, on ne sait peut-être pas ou il n'est peut-être pas certain qu'il s'agit d'un incident de biosûreté; celui-ci peut être délibérément caché s'il est intentionnel. Ainsi, les éléments de biosûreté devraient être pris en considération dans l'approche « tous risques » liée à l'enquête sur les incidents de façon à ne pas omettre d'éléments de preuve importants. L'enquête sur les incidents devrait tenir compte de la possibilité que les preuves d'actes intentionnels puissent être délibérément cachées. À moins que les preuves démontrent le contraire, les facteurs liés à la biosûreté ne devraient pas être écartés. S'il existe une possibilité

qu'un incident découle d'un acte criminel, il peut être prudent d'obtenir aux premières étapes l'aide des autorités responsables de l'application de la loi.

Le processus d'enquête sur les incidents est systématique et comprend généralement les étapes présentées ci-dessous, qui sont décrites en détail au chapitre 18 du GCB.

- Intervention initiale;
- Collecte des éléments de preuve et des renseignements;
- Analyse et détermination des causes fondamentales;
- Élaboration de plans de mesures correctives et préventives;
- Évaluation et amélioration continue.

L'enquête sur les incidents de biosûreté est peut-être déjà décrite dans les PON sur les enquêtes d'incidents sur la biosécurité, qui sont incluses dans le Manuel de biosécurité, ou qui peuvent être élaborées comme PON distinctes, spécifiques à la biosûreté. Comme pour les autres PON, elles devraient être révisées et mises à jour régulièrement. Une personne responsable de cette tâche devrait être désignée.

Selon la nature et la gravité de l'incident, on peut confier l'enquête à une seule personne ou mettre sur pied une équipe dans les situations plus complexes. La ou les personnes devraient mener l'enquête en ayant l'esprit ouvert, sans aucun a priori concernant l'incident. La portée et l'ampleur de l'enquête sur un incident peuvent varier selon la gravité de l'incident.

Références

1 Gouvernement du Canada. (2016). *Guide canadien sur la biosécurité*, 2e éd., Ottawa, ON, Canada : Gouvernement du Canada.

2 Gouvernement du Canada. (2015). *Norme canadienne sur la biosécurité*, 2e éd., Ottawa, ON, Canada : Gouvernement du Canada.

GESTION ET SÉCURITÉ DE L'INFORMATION



CHAPITRE 7 - GESTION ET SÉCURITÉ DE L'INFORMATION

La façon dont les ressources en matière d'information liées aux agents pathogènes et aux toxines sont protégées fait partie intégrante d'un plan de biosûreté. De nombreux types de renseignements que possède une installation peuvent être considérés comme des ressources exigeant une protection contre la perte, le vol, les dommages ou la diffusion. La sécurité de l'information vise à protéger les renseignements, en gardant confidentiels les renseignements de nature délicate (p. ex. les renseignements sur les ABCSE et les toxines présents dans l'installation), en maintenant l'intégrité de tous les renseignements, et en rendant ceux-ci accessibles uniquement aux personnes qui en ont besoin.

La sécurité de l'information vise à protéger les ressources en matière d'information dans tous les formats, qu'il s'agisse de formats papier, de documents électroniques ou de connaissances conservées par le personnel, tout en permettant l'accès autorisé uniquement aux personnes qui en ont besoin. Une évaluation de la sécurité de l'information tient compte des personnes qui doivent avoir accès aux renseignements et des méthodes utilisées pour protéger les renseignements qui sont proportionnels aux risques de biosûreté. Des éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté associés à la sécurité de l'information se trouvent dans le tableau 7-1.

7.1 Ressources en matière d'information

Les ressources en matière d'information peuvent fournir des renseignements sur les agents pathogènes humains, les agents zoopathogènes, les toxines et autres matières infectieuses réglementées qui doivent être protégés. Comme pour les autres ressources, ces renseignements doivent être définis et classés selon leur valeur (notamment leur criticité et leur vulnérabilité à la compromission ou à leur diffusion) à l'aide du processus d'évaluation des risques de biosûreté décrit au chapitre 6 du GCB.

Savoir quelle information doit être protégée et à quel niveau aide à maintenir la sensibilisation des employés au sujet des renseignements qu'ils ont la responsabilité de protéger. En ce qui concerne la biosûreté, les ressources en matière d'information peuvent comprendre ce qui suit :

- inventaires;
- évaluation des risques de biosécurité et de biosûreté;
- protocoles et résultats expérimentaux;
- information scientifique et exclusive (p. ex. les processus, les techniques, les séquences des gènes);
- autorisations d'accès et registres;
- plans des bâtiments;
- dossiers du personnel et documents financiers;
- inventaires des matières biologiques et emplacements des aires d'entreposage.

La NCB exige qu'une description du plan de biosûreté figure dans le Manuel de biosécurité. Cependant, il se peut que le plan de biosûreté détaillé et les évaluations des risques de biosûreté doivent demeurer confidentiels étant donné qu'ils renferment des renseignements confidentiels (p. ex. sur les systèmes de sécurité, le personnel, les agents pathogènes, les procédures).

7.2 Classification des renseignements

La classification des renseignements aidera à déterminer le niveau de sécurité nécessaire. Les catégories sont fournies uniquement à titre d'exemple. Les organisations peuvent déjà posséder un système de classification ou peuvent choisir de modifier les catégories suggérées. Il faut noter également que certains renseignements peuvent être assujettis aux lois fédérales, provinciales ou territoriales sur la protection de la vie privée (p. ex. les renseignements personnels).

- Public – renseignements destinés au grand public, avec l'approbation appropriée
- Interne – renseignements non destinés au grand public. Les analyses de données et les ébauches de documents communiqués aux autres membres du personnel aux fins d'examen en sont des exemples
- Accès limité ou restreint – renseignements destinés uniquement aux personnes autorisées. La diffusion de renseignements peut avoir une incidence négative sur les personnes, par exemple les PON et les données d'études
- Confidentiel – renseignements destinés uniquement à un petit nombre de personnes autorisées qui ont besoin de savoir. La diffusion de renseignements peut compromettre la sécurité de l'installation ou des systèmes de confinement critiques. Parmi les exemples, mentionnons la recherche sur le gain de fonction et la **possibilité d'un double usage**, les informations exclusives critiques et les détails sur les systèmes de sécurité

La classification des renseignements peut varier d'une organisation à une autre. La façon de la mettre en œuvre est laissée à la discrétion de l'organisation, car elle dépend du type de renseignements détenus. Les données considérées comme restreintes par une organisation peuvent être considérées comme confidentielles par une autre. Les renseignements qui exigent des mesures de sécurité plus élevées peuvent entraîner des coûts importants (p. ex. coûts liés au matériel, aux logiciels et à la facilité d'accès). Les dommages découlant de la compromission des renseignements devraient être évalués par rapport aux coûts liés à la mise en place de stratégies d'atténuation.

7.3 Sécurité des renseignements

Des mesures efficaces de sécurité des renseignements devraient protéger les ressources en matière d'information de forme électroniques et non électroniques, de leur création jusqu'à leur transfert, destruction, épuration ou élimination, y compris pendant l'entreposage ou le transfert de l'information. Certaines installations préfèrent peut-être conserver les mesures de sécurité des renseignements dans un plan distinct. Dans ce cas, une description des mesures de sécurité mises en place doit être incluse dans le plan de biosûreté. Le succès d'un plan de sécurité des renseignements dépend largement de l'appui de la direction. Élaborer, mettre en

place et maintenir des mesures de sécurité des renseignements exigent des ressources (du personnel, des fonds), ainsi que l'adhésion de tout le personnel.

Dans les deux cas, une personne ou une équipe devrait se charger de la sécurité des renseignements de façon que les menaces potentielles et les mesures de sécurité puissent être revues régulièrement (p. ex. révision mensuelle, semestrielle ou annuelle). Cela comprend notamment ce qui suit : se tenir au courant des dernières menaces (p. ex. attaques par ingénierie sociale, maliciels, pourriels, hameçonnage, piratage); mettre en place les contremesures les plus à jour (p. ex. installation d'un logiciel antivirus et de coupe-feux); aviser le personnel des tentatives d'hameçonnage; exiger le changement fréquent des mots de passe si un ou plusieurs bris se sont produit dans le passé).

Tableau7-1 : Éventuelles mesures qui peuvent être mises en œuvre pour atténuer les risques de biosûreté liés à la sécurité des renseignements dans un NC2, un NC3 et une zone d'ABCSE

Élément du plan de biosûreté	Risque	Éventuelles mesures d'atténuation des risques		
		NC2	NC3	Zone d'ABCSE
Sécurité des renseignements	La violation des données conservées sur un réseau partagé.	• L'information concernant le laboratoire conservée sur un réseau partagé est sauvegardée dans un fichier à contrôle d'accès accessible par le personnel de laboratoire (p. ex. par un compte d'utilisateur générique de l'installation).	• Le réseau partagé est uniquement accessible avec un nom d'utilisateur et un mot de passe. • L'information concernant le laboratoire conservée sur un réseau partagé est sauvegardée dans un fichier à accès restreint seulement accessible par le personnel autorisé.	• Le réseau partagé est uniquement accessible par authentification à deux facteurs (p. ex. nom d'utilisateur individuel et mot de passe utilisés en association avec une clé, une carte GRID ou empreinte digitale). • Les fichiers sensibles à accès restreint sont cryptés ou sauvegardés en dehors du réseau partagé. • L'information concernant le laboratoire conservée sur un réseau partagé est sauvegardée dans un fichier à accès restreint seulement accessible par le personnel autorisé détenant une Habilitation de sécurité en vertu de la LAPHT valide. • L'accès à distance aux fichiers contenant des registres sur des ABCSE est bloqué. • L'historique de l'accès et des changements aux fichiers à accès restreint est enregistré par un journal d'audit électronique.

	Perte d'une clé USB contenant des données de laboratoire	• Politique et procédure limitant l'utilisation des clés USB.	• Politique et procédure limitant l'utilisation des clés USB et exigeant l'utilisation de mot de passe pour protéger les documents. • La perte de clés USB doit être déclarée à l'ASB.	• Politique et procédure limitant l'utilisation des clés USB et exigeant l'approbation pour chaque utilisation. • Utilisation de clés USB cryptées. • La perte de clés USB doit être déclarée à l'ASB et au service de sécurité.
--	--	---	---	--

7.3.1 Politiques et normes

Des politiques peuvent être établies afin de régir l'identification, la classification (p. ex. les informations exclusives, confidentielles ou à accès restreint) et la manipulation des renseignements de nature délicate, et de dicter la façon dont les renseignements doivent être recueillis, consignés, transmis, entreposés, consultés et détruits. Les politiques sur l'utilisation de l'Internet et l'utilisation des supports de données amovibles (p. ex. les clés USB) peuvent fournir au personnel de l'information claire sur les attentes relatives à leur utilisation. Les bonnes politiques sont simples et directes. Par exemple, l'accès à distance (p. ex. à partir de la maison) au réseau de l'installation est seulement autorisé à partir d'un ordinateur portable de l'installation équipé d'un logiciel antivirus mis à jour, en exigeant des mots de passe très sûrs, et en interdisant qu'on écrit les mots de passe dans des endroits facilement accessible. Des ententes de non-divulgaration peuvent être prises afin d'interdire au personnel de discuter ou de diffuser des renseignements exclusifs ou de nature délicate.

7.3.2 Information sur papier

La mise en œuvre d'une politique de « bureau dégagé » qui exige du personnel qu'il classe et protège de façon appropriée (p. ex. dans un tiroir de bureau sous clé, un classeur de bureau, un classeur de sécurité, un coffre-fort ou autre meuble protégé, le cas échéant) les documents de nature délicate, ce qui comprend les cahiers de laboratoire, les mots de passe, les données et les PON, empêchera leur accès par des personnes non autorisées. De plus, l'établissement de politiques et de procédures sur les situations où le personnel doit transporter des documents de nature délicate et utiliser les technologies de reproduction (p. ex. photocopieurs, numériseurs, caméras, appareils et téléphones mobiles) aidera également à protéger l'information en format papier. Les renseignements de nature délicate devraient être imprimés au poste de travail et enlevés de l'imprimante immédiatement après leur impression, ou imprimés à l'aide d'une option d'impression sécurisée (locked print) dans le cas d'une imprimante centralisée.

7.3.3 Information sur les ABCSE

Limiter au personnel autorisé l'accès aux registres et aux documents relatifs aux activités réglementées comportant la manipulation d'agents pathogènes humains des GR3 et GR4, des toxines et ABCSE constitue une exigence (matrice 4.10 de la NCB). Cette exigence s'étend à toute personne qui pourrait avoir accès à de l'information électronique. Une Habilitation de sécurité en vertu de la LAPHT n'est pas exigée du personnel ayant accès à de l'information relative à des ABCSE ou contrôlant ces derniers, comme les administrateurs de TI. Cependant, les installations devraient envisager de mettre en place une politique faisant en sorte que seules les personnes autorisées aient accès à l'information. Les installations qui désirent obtenir une Habilitation de sécurité en vertu de la LAPHT pour ces personnes sur une base volontaire peuvent soumettre leur demande à l'ACSP.

La nature délicate de l'information et des applications à double usage devrait être prise en considération lors de la présentation d'études liées aux ABCSE dans des publications scientifiques (p. ex. la procédure de clonage pour reconstituer un virus disparu). Cependant, ces questions dépassent la portée du présent guide¹.

7.3.4 Sécurité de l'information électronique

La sécurité des TI fait plus particulièrement référence à la protection de l'information électronique, comme les renseignements emmagasinés dans des ordinateurs personnels, des serveurs ou des supports amovibles, ou de l'information transférée électroniquement, ce qui comprend l'infonuagique, qui peut nécessiter des mesures de sécurité supplémentaires². Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) de Sécurité publique Canada offre divers documents d'orientation, bulletins de sécurité et rapports techniques portant sur des questions de cybersécurité, notamment sur les alertes et les avis pour communiquer des renseignements sur des menaces, des vulnérabilités ou des incidents potentiels, imminents ou réels, pouvant toucher l'infrastructure essentielle du Canada³.

Selon les exigences en matière de sécurité de l'information, il peut être acceptable de conserver de l'information sur un réseau protégé. Cependant, l'information de nature délicate est conservée de façon plus sécuritaire si elle est cryptée sur un support amovible (p. ex. sur un CD-ROM ou une clé USB), ou si elle est conservée en format papier uniquement, dans un lieu sûr, accessible seulement aux personnes autorisées. Cette information ne devrait jamais être emmagasinée sur un réseau ouvert ou partagée sans une protection appropriée. Le lieu choisi pour conserver les documents ne devrait être accessible qu'aux personnes qui ont besoin d'en prendre connaissance (« besoin de savoir »), comme il a été déterminé par l'organisation (p. ex. l'ASB, un directeur, un superviseur). L'aire d'entreposage devrait être suffisamment protégée contre les dommages ou la perte d'information. Les documents contenant des renseignements de nature délicate qui sont désuets ou qui ne sont plus pertinents devraient être déchiquetés ou détruits, conformément à leur cote⁴.

En plus de l'information elle-même, d'autres aspects de la sécurité de l'information doivent être pris en considération. Les supports amovibles, comme les clés USB, peuvent être facilement égarés et les ordinateurs portatifs peuvent devenir une proie facile pour les voleurs. Même si l'information qu'ils contiennent peut s'avérer difficile d'accès aux personnes non

autorisées, celle-ci pourrait être irremplaçable et sa perte avoir des répercussions sur l'organisation (p. ex. les inventaires, la liste des personnes autorisées à pénétrer dans une zone de confinement).

Les appareils ou dispositifs couramment utilisés qui peuvent facilement être cachés à la vue ou qui sont considérés comme inoffensifs (p. ex. les téléphones cellulaires intelligents, les assistants numériques personnels [ANP], les clés USB, les cartes mémoires SD) présentent une vulnérabilité à la sécurité de l'information. La préoccupation liée à ces appareils réside dans leur capacité à emmagasiner une grande quantité d'information sur un support minuscule, amovible, qui peut facilement être transporté à l'extérieur d'une installation sans être détecté. De plus, le transfert de fichiers d'un ordinateur domestique à un ordinateur utilisé au travail peut introduire un logiciel malveillant. L'installation devrait envisager d'inclure ces types d'appareils dans ses politiques sur la sécurité de l'information, reconnaissant qu'ils peuvent être utilisés à mauvais escient, dans le but d'atténuer ce risque à un niveau acceptable.

Les points suivants relatifs à l'utilisation de l'information électronique peuvent être pris en considération dans l'établissement des politiques ou des normes.

7.3.4.1 Sécurité générale de l'information électronique

- Mettre en place une politique claire de surveillance visant à verrouiller l'écran ou à fermer la session sur l'ordinateur ou le terminal lorsque celui-ci n'est pas utilisé, afin d'empêcher les personnes non autorisées d'accéder à l'ordinateur.
- Utiliser des dispositifs de protection à l'écran de l'ordinateur ou du terminal afin d'empêcher que l'information affichée soit vue par des collègues ou par des intrus à travers une fenêtre.
- Verrouiller les documents électroniques de nature délicate pour les mettre « en lecture seule » pour éviter qu'ils soient modifiés.
- Comprendre le type d'information qui peut être partagé afin de prévenir la transmission de cette information à des personnes non autorisées.
- Mettre en place une politique relative à l'utilisation acceptable des ordinateurs et de l'Internet, et à l'installation de logiciels pour éviter toute introduction involontaire de logiciels malveillants, de virus et de logiciels espions.
- Limiter l'utilisation d'ordinateurs portatifs et le télétravail, par exemple éviter l'utilisation de réseaux sans fil non protégés, et utiliser uniquement des dispositifs de protection antivirus pour l'accès à distance afin de protéger l'ordinateur et le réseau local.
- Utiliser des méthodes de transfert de l'information sécurisé, par exemple des fichiers protégés par des mots de passe ou le chiffrement électronique pour l'envoi de courriel, ou le télécopieur, pour éviter que des fichiers soient envoyés à la mauvaise adresse.
- Installer les ordinateurs et les serveurs dans une aire protégée, comme le placard du réseau local mis sous clé ou une salle d'ordinateurs ou de serveurs verrouillée. Authentifier l'identité de l'utilisateur avant d'accorder l'accès. En fonction des besoins de sécurité (p. ex. il peut s'agir d'une authentification au moyen d'un seul facteur qui nécessite un nom d'utilisateur et un mot de passe très sûr, ou d'une authentification à deux facteurs qui exige également l'utilisation d'un objet physique que possède l'utilisateur (p. ex. clé, carte d'authentification [grid], clé USB), ou des caractéristiques physiques de l'utilisateur (p. ex. empreinte digitale, voix, oeil).

- Utiliser des réseaux sécurisés, y compris des fournisseurs tierce partie cautionnés, dignes de confiance.
- Utiliser un réseau privé virtuel (VPN) pour communiquer entre les bureaux ou locaux comparables, le cas échéant.

7.3.4.2 Sécurité du réseau local

- Mettre en place une politique sur les mots de passe (créer des mots de passe très sûrs et définir la fréquence de changement de ces derniers).
- Installer un pare-feu de réseau pour contrer le pollupostage et les logiciels malveillants.
- Mettre à jour régulièrement le logiciel antivirus.
- Restreindre l'accès aux lecteurs et aux dossiers du réseau aux personnes chargées d'améliorer la sécurité des dossiers de nature délicate.

7.3.4.3 Internet

- Ne visiter que les sites fiables, dignes de confiance. Même si des sites Web particuliers peuvent être bloqués par un pare-feu, les administrateurs devront ajouter continuellement de nouveaux sites à la liste pour qu'elle soit efficace.
- Établir des politiques sur l'utilisation du stockage en ligne (p. ex. le stockage infonuagique) et les applications.
- Vérifier l'adresse des pages Web, ou copier et coller le lien dans le navigateur, plutôt que de simplement cliquer sur celui-ci.
- Utiliser des logiciels de sécurité Internet.
- Ne pas modifier ou désactiver les mesures de sécurité, comme le logiciel antivirus.
- Ne fournir des renseignements personnels ou de nature délicate qu'à une source protégée, fiable (p. ex. effectuer un achat par carte de crédit seulement sur la page Web sécurisée du vendeur).
- Mettre à niveau les logiciels, au besoin, de façon à ce que toutes les corrections de sécurité et les définitions antivirus soient à jour.
- Installer un pare-feu.
- Utiliser les options administratives afin d'intégrer les filtres permettant de restreindre l'accès aux sites Web externes (l'accès filtré par rapport à l'accès non filtré avec accès à la personne autorisée seulement).

7.3.4.4 Courrier électronique

- Établir des politiques sur la gestion du courrier électronique.
- Installer un filtre anti-pourriel.
- Ne pas cliquer sur des liens à partir d'un courriel.
- Mettre en place des normes strictes relatives aux mots de passe des comptes de courrier électronique.
- Ne pas transférer à d'autres personnes des courriels potentiellement malveillants.

- Tenir les employés au courant de l'information qu'ils sont autorisés à envoyer par courriel.
- Si des fichiers doivent être envoyés par courrier électronique, recourir au chiffrement.

7.3.4.5 Données

- Sauvegarder les données sur un disque dur externe sécurisé ou un serveur distant pour éviter les pertes potentielles. Cette méthode protège également contre les interruptions accidentelles (p. ex. les défaillances de matériel). La fréquence de la sauvegarde dépendra de la fréquence à laquelle les documents sont modifiés.
- Incorporer une fonction de sauvegarde automatique dans le logiciel.

7.3.4.6 Accès à distance

- Idéalement, la personne ayant accès au réseau de l'installation à partir d'un emplacement distant devrait utiliser une connexion directe au routeur (câble Ethernet). Si un accès sans fil est utilisé, n'utiliser qu'un accès sans fil sécurisé et activer le chiffrement.
- Limiter l'accès à l'ordinateur servant à l'accès à distance (p. ex. les enfants et les visiteurs ne devraient pas être autorisés à utiliser l'ordinateur).

7.3.4.7 Téléphones et autres dispositifs mobiles

- Traiter les téléphones et autres dispositifs mobiles en prenant les mêmes mesures de précaution que celles d'un ordinateur de bureau ou d'un ordinateur portable.
- Utiliser l'option de mot de passe d'accès au système, et laisser le dispositif verrouillé lorsqu'il n'est pas utilisé.
- Utiliser les caractéristiques de sécurité du dispositif et installer un logiciel antimaliciels, lorsque c'est possible.
- Sauvegarder régulièrement l'information emmagasinée sur le dispositif.

7.3.4.8 Dispositifs de stockage des données

- Mettre en place des politiques sur l'utilisation et le transport des dispositifs de stockage électroniques amovibles, comme les clés USB, les cartes à mémoire SD et les disques durs mobiles.

7.3.4.9 Appareils photo et dispositifs d'enregistrement vidéo

- Mettre en place des politiques sur l'utilisation des appareils photo et des dispositifs d'enregistrement vidéo (ce qui comprend les téléphones intelligents et cellulaires) et la publication et la diffusion de ce type d'information.

Références

- 1 Tumpey T, Basler C, Aguilar P, Zeng H, Solórzano A, Swayne D, Cox N, Katz J, Taubenberger J, Palese P, García-Sastre A. (2005). Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus. *Science*, 310(5745):77-80.
- 2 Gouvernement du Canada. (2013). *Guide Pensez cybersécurité pour les petites et moyennes entreprises*. Ottawa, ON, Canada : Sécurité publique Canada.
Consulté le 8 février 2016 à l'adresse <http://www.pensezcybersecurite.gc.ca/cnt/rsrscs/pblctns/sml-bnss-gd/index-fr.aspx>
- 3 Gouvernement du Canada. (2015). *Centre canadien de réponse aux incidents cybernétiques*. Consulté le 8 février 2016 à l'adresse <http://www.securitepublique.gc.ca/cnt/ntnl-scr/cbr-scr/ccirc-ccric-fr.aspx>
- 4 .Gendarmerie royale du Canada. (2014). *Sélection de l'équipement de destruction- section 2*. Consulté le 8 février 2016 à l'adresse http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/page_0068_f.htm

MISE EN ŒUVRE, ÉVALUATION ET AMÉLIORATION DU PLAN DE BIOSÛRETÉ



CHAPITRE 8 - MISE EN ŒUVRE, ÉVALUATION ET AMÉLIORATION DU PLAN DE BIOSÛRETÉ

Un plan de biosûreté doit être élaboré, mis en œuvre, révisé et amélioré au besoin, et tenu à jour. La mise en œuvre comprend l'installation et la mise à l'essai des mesures de sécurité physique, mais également la formation initiale du personnel sur les politiques et les procédures, et la sensibilisation continue à la biosûreté.

L'évaluation de l'efficacité du plan de biosûreté de façon régulière, lorsque des changements surviennent qui peuvent avoir une incidence sur la biosûreté, et en réaction à des incidents de biosûreté, aidera à cerner les vulnérabilités et les secteurs à améliorer.

8.1 Formation

La formation est un élément clé de la biosécurité et de la biosûreté, et essentiel au succès du programme de biosécurité. Le personnel doit bien connaître les risques, y compris toutes les menaces de biosûreté associées aux agents pathogènes et aux toxines présents dans son environnement de travail, les pratiques et les outils qui peuvent prévenir l'exposition accidentelle à des agents pathogènes et des toxines, ou leur libération accidentelle, et veiller à la sécurité des ressources. La formation peut porter sur les besoins particuliers de la personne, les tâches particulières qu'elle exécute et les risques posés par les agents pathogènes et les toxines manipulés ou entreposés dans l'installation. Le chapitre 8 du GCB fournit de plus amples renseignements au sujet de la formation sur la biosécurité.

Avant qu'une personne se voie accordé l'accès à des agents pathogènes et des toxines, il est important que celle-ci comprenne et suive tous les protocoles de biosûreté (y compris la sécurité de l'information) établis par l'installation. Les éléments de biosûreté devraient être intégrés au programme de formation existant et diffusés à toutes les personnes autorisées à pénétrer dans une zone de confinement. Il est recommandé d'inclure dans la formation sur la biosûreté des modules sur les procédures et les processus particuliers liés à la sécurité qui contrôlent l'accès et préviennent la perte, le vol ou la compromission d'agents pathogènes, de toxines et autres ressources. Une formation d'appoint devrait être offerte à une fréquence déterminée par l'évaluation des besoins de formation ou lorsque des changements aux processus ou aux procédures sont mis en œuvre.

8.1.1 Sensibilisation à la biosûreté

La formation de sensibilisation à la biosûreté fournit au personnel une compréhension claire des rôles et des responsabilités, et établit des attentes claires en ce qui concerne les façons de protéger les ressources de l'installation. Cette formation est un élément important du programme d'évaluation de la fiabilité continue visant à détecter et à contrer d'autres menaces internes et externes. La sensibilisation à la biosûreté devrait :

- fournir au personnel une formation visant à reconnaître, à comprendre les répercussions éventuelles et à signaler les activités suspectes, par exemple :
 - utilisation de fausses pièces d'identité;
 - comportement suspect;
 - clés, carte-clés ou matériel perdus ou volés;
 - comportement dangereux.
- présenter les politiques et les procédures de l'organisation visant à protéger les renseignements de nature délicate;
- inclure une formation sur les techniques et les indicateurs permettant de détecter toute activité suspecte et tout changement de comportement chez le personnel ou les visiteurs;
- informer le personnel des conséquences d'un comportement inapproprié;
- donner des instructions sur les pratiques et les procédures en matière de sécurité, et sur le signalement d'événements suspects et d'incidents liés à la sécurité.

Les sujets recommandés dans le cadre de la formation portant sur la sensibilisation à la biosûreté comprennent ce qui suit¹ :

- identification des personnes suspectes et intervention (signalement, expulsion);
- reconnaissance des menaces internes;
- procédures d'accompagnement et de supervision;
- formation d'appoint sur la procédure d'intervention en cas d'urgence (matrice 4.3 du GCB);
- examen des rapports d'incident au sein de l'établissement ou mentionné dans des publications afin de mettre à profit les leçons retenues.

Les activités continues de sensibilisation à la biosûreté peuvent informer le personnel des menaces récentes, telles que les tentatives d'accès non autorisé ou un nouveau virus informatique, tout en faisant un rappel de leurs responsabilités.

8.1.1.1 Ingénierie sociale

L'ingénierie sociale est souvent une des nombreuses étapes dans une fraude complexe. Les criminels utilisent l'ingénierie sociale pour obtenir de l'information (p. ex. des renseignements personnels, des mots de passe) qui peut être utilisée pour accéder à des ressources ou à des

renseignements confidentiels. Elle est utilisée en raison de son efficacité. La formation devrait informer le personnel qu'il doit :

- faire preuve de prudence à l'égard d'une personne qui demande des renseignements sur un membre du personnel, sa famille, ou des renseignements de nature délicate;
- demander à toutes les personnes qui font des demandes inhabituelles de confirmer leur identité à l'aide de documents officiels;
- signaler toute activité suspecte à la direction.

8.1.1.2 Sensibilisation à la sécurité de l'information

Un programme de sensibilisation à la sécurité tiendra le personnel informé des pratiques, des politiques et des normes de sécurité de l'installation. La sécurité de l'information devrait être incluse dans la formation, mais la sensibilisation de la sécurité de l'information nécessite plus qu'une simple formation. Bien que le sujet de la sécurité de l'information puisse être présenté à un niveau de base dans une formation initiale sur la sensibilisation à la sécurité, celle-ci devrait être élargie au fil du temps pour inclure une formation plus approfondie. Le personnel devrait recevoir des mises à jour et des rappels réguliers afin de maintenir le niveau de sensibilisation et d'accroître celle-ci lorsque les circonstances le justifient.

8.2 Entretien et vérification des systèmes de sécurité

Il est essentiel que tout l'équipement et toutes les procédures servant à maintenir une barrière de sécurité physique, y compris la barrière physique elle-même, soient inspectés régulièrement afin de vérifier qu'ils remplissent leur fonction efficacement. Tous les systèmes de contrôle d'accès, les systèmes de détection d'intrusion et les dispositifs de verrouillage devraient être installés, exploités et entretenus conformément aux spécifications du fabricant. La performance des dispositifs de détection d'intrusion devrait être vérifiée régulièrement (p. ex. mensuellement, semestriellement, annuellement), en fonction de l'évaluation des risques, afin de confirmer leur fonctionnement continu effectif. Un registre des essais de performance devrait être conservé au dossier. La vérification des systèmes électroniques devrait également être effectuée durant une panne de courant, ou le protocole d'urgence pour ce genre de situation devrait être révisé.

8.3 Évaluation et amélioration continue du plan de biosûreté

Le plan de biosûreté devrait être régulièrement révisés et amélioré de façon continue par la personne investie d'un pouvoir délégué relatif à la biosûreté pour permettre de vérifier que le plan demeure pertinent, applicable et efficace. La période d'examen dépendra des risques de biosûreté. Par exemple, dans le cas du confinement de niveau le plus faible (c.-à-d. NC2), il peut s'agir simplement confirmer que les risques de biosûreté demeurent inchangés (p. ex. il n'y a aucun changement concernant les agents pathogènes et les toxines manipulés ou entreposés) et qu'aucun incident de biosûreté ne s'est produit durant la période d'examen, alors qu'un examen approfondi du plan de biosûreté est nécessaire toutes les fois que

l'évaluation des risques de biosûreté fait l'objet d'un examen. De plus, le plan de biosûreté devrait être examiné à la suite d'un incident et mis à jour en fonction de la détermination des causes profondes.

La haute direction peut également examiner le plan de biosûreté à intervalles réguliers afin de confirmer que le plan existant répond aux besoins de l'établissement ou de l'organisation et continue de refléter les buts et les objectifs à long terme.

L'examen aidera à répondre aux questions générales liées à la biosûreté, par exemple :

- Le plan actuel répond-il aux besoins de l'installation?
- Les six éléments de la biosûreté sont-ils pris en compte de façon appropriée?
- Les procédures et les processus sont-ils tous mis en œuvre de façon appropriée?
- Le personnel est-il adéquatement formé sur la biosûreté?
- Le plan doit-il être mis à jour (p. ex. en réponse au changement ou aux événements)?
- Des ressources adéquates sont-elles disponibles pour maintenir la biosûreté?

Toutes les questions touchant la biosûreté, relevées durant l'examen, doivent être prises en compte en mettant à jour le plan ou en mettant en œuvre de nouvelles procédures.

Références

¹ Centers for Disease Control and Prevention des États-Unis, Division of Select Agents and Toxins et Animal and Plant Health Inspection Service Agriculture Select Agent Program. (2013). *Security Guidance for Select Agent or Toxin Facilities* (2nd Revision). Consulté le 8 février 2016 à l'adresse http://www.selectagents.gov/resources/Security_Guidance_v3-English.pdf

GLOSSAIRE



CHAPITRE 9 - GLOSSAIRE

Il est important de souligner que, même si certaines des définitions fournies dans le glossaire sont universellement reconnues, beaucoup d'entre elles ont été établies expressément pour la NCB, le GCB et la *Ligne directrice canadienne sur la biosécurité : Élaboration d'un plan de biosûreté exhaustif*; par conséquent, certaines définitions pourraient ne pas s'appliquer aux installations qui ne sont pas visées par la NCB et le GCB.

Accès limité	Permission d'accès accordée uniquement aux personnes et aux visiteurs autorisés. Pour ce faire, on a recours à un moyen opérationnel (p. ex. la surveillance régulière des personnes autorisées, le contrôle de toutes celles qui accèdent à une zone désignée) ou à une barrière physique (p. ex. un système de contrôle d'accès tel que des serrures à clé ou des cartes d'accès électroniques).
Accès restreint	Permission d'accès accordée exclusivement aux personnes autorisées en ayant seulement recours à une barrière physique (c.-à-d. à un dispositif ou à un système de contrôle d'accès tels que des cartes d'accès électroniques ou des codes d'accès).
Accident	Événement imprévu ayant causé des blessures, un préjudice ou des dommages.
Activité réglementée	Activité visée par le paragraphe 7(1) de la <i>Loi sur les agents pathogènes humains et les toxines</i> , à savoir : posséder, manipuler ou utiliser des agents pathogènes humains ou des toxines; les produire; les entreposer; permettre à quiconque d'y avoir accès; les transférer; les importer ou les exporter; les rejeter ou les abandonner de toute autre manière; les éliminer.
Agent de la sécurité biologique (ASB)	Personne désignée pour superviser les pratiques en matière de biosécurité et de biosûreté dans une installation.
Agent pathogène	Microorganisme, acide nucléique ou protéine ayant la capacité de causer une maladie ou une infection chez l'humain ou l'animal. Des exemples d'agents pathogènes humains figurent aux annexes 2 à 4 et à la partie 2 de l'annexe 5 de la <i>Loi sur les agents pathogènes humains et les toxines</i> , mais ils ne constituent pas une liste exhaustive; des exemples d'agents zoopathogènes peuvent être trouvés à l'aide du Système automatisé de référence à l'importation sur le site Web de l'Agence canadienne d'inspection des aliments.

Agent zoopathogène	Agent qui cause des maladies chez les animaux, qu'il soit issu de la biotechnologie ou non. Dans la <i>Norme canadienne sur la biosécurité</i> et le <i>Guide canadien sur la biosécurité</i> , le terme « agent zoopathogène » ne fait référence qu'à un agent qui cause des maladies chez les animaux terrestres, y compris chez les oiseaux et les amphibiens; toutefois, ce terme ne s'applique pas aux agents qui causent des maladies chez les animaux aquatiques ou les invertébrés.
Agents biologiques à cote de sécurité élevée (ABCSE)	Sous-ensemble d'agents pathogènes humains et de toxines qui présentent un risque accru en matière de biosûreté en raison de la possibilité qu'on les utilise comme arme biologique. Au paragraphe 10 du <i>Règlement sur les agents pathogènes humains et les toxines</i> , les ABCSE sont identifiés comme des agents pathogènes et des toxines « précisés ». Les ABCSE comprennent donc tous les agents pathogènes du groupe de risque 3 et du groupe de risque 4 qui se retrouvent sur la <i>Liste des agents pathogènes humains et animaux et des toxines réglementés à l'exportation</i> , publiée par le Groupe d'Australie et sujette à modifications, à l'exception du virus Duvenhage, du virus rabique et de tous les autres du genre <i>Lyssavirus</i> , du virus de la stomatite vésiculaire ainsi que du virus de la chorioméningite lymphocytaire. Les ABCSE comprennent aussi toutes les toxines qui se trouvent à la fois à l'annexe 1 de la <i>Loi sur les agents pathogènes humains et les toxines</i> et sur la <i>Liste des agents pathogènes humains et animaux et des toxines réglementés à l'exportation</i> , et qui sont présentes en quantités supérieures aux quantités seuils énoncées au paragraphe 10(2) du <i>Règlement sur les agents pathogènes humains et les toxines</i> .
Barrière de sécurité	Obstacle physique conçu pour empêcher les personnes non autorisées d'avoir accès aux agents pathogènes, aux matières infectieuses, aux toxines et aux autres ressources de l'installation (p. ex. portes verrouillées, systèmes de contrôle d'accès, équipement d'entreposage cadenassé). La barrière de sécurité rend la zone de confinement plus sécuritaire en limitant l'accès aux personnes autorisées seulement.
Biosécurité	Ensemble des principes, des technologies et des pratiques liés au confinement mis en œuvre pour prévenir l'exposition involontaire à des matières infectieuses et à des toxines, ou leur libération accidentelle.
Biosûreté	Ensemble des mesures visant à prévenir la perte, le vol, le mésusage, le détournement ou la libération intentionnelle d'agents pathogènes, de toxines ou d'autres ressources liés à l'installation (p. ex. le personnel, l'équipement, les matières non infectieuses, les animaux).
Communauté	Englobe à la fois la population humaine (c.-à-d. le public) et la population animale.

Confinement	Ensemble de paramètres de conception physique et de pratiques opérationnelles visant à protéger le personnel, le milieu de travail immédiat et la communauté contre toute exposition à des matières biologiques. Dans le même contexte, on utilise aussi le terme « bioconfinement ».
Déplacement	Fait de déplacer (p. ex. amener ou apporter, manutentionner, conduire, relocaliser) des personnes, des matières (y compris les matières infectieuses et les toxines) ou des animaux d'un emplacement à un autre, dans un même bâtiment. Le déplacement peut se faire de différentes manières : à l'intérieur d'une même zone de confinement; vers un autre emplacement dans le même bâtiment; vers une autre zone de confinement située dans le même bâtiment.
Entreposage à long terme	Fait de posséder des matières (c.-à-d. des agents pathogènes, des toxines ou d'autres matières infectieuses réglementées) plus de 30 jours après leur réception ou leur création, selon l'usage de la <i>Norme canadienne sur la biosécurité</i> et du <i>Guide canadien sur la biosécurité</i> .
Espace de travail en laboratoire	Aire située à l'intérieur d'une zone de confinement, conçue et équipée de façon à ce qu'on puisse y mener des activités de diagnostic, d'enseignement ou de recherche <i>in vitro</i> .
Évaluation des risques de biosûreté	Évaluation des risques qui consiste à répertorier et à classer par ordre de priorité les agents pathogènes, les toxines, les matières infectieuses et les autres ressources (p. ex. l'équipement, les animaux, les renseignements) présents dans une installation, à définir les menaces et les risques associés à ces matières, ainsi qu'à déterminer les stratégies d'atténuation appropriées afin de prévenir le vol, le mésusage, le détournement ou la libération intentionnelle de ces matières.
Évaluation locale des risques (ELR)	Évaluation propre à un endroit en particulier réalisée pour repérer les dangers associés aux activités menées ainsi qu'aux matières infectieuses ou aux toxines utilisées. Cette évaluation permet d'élaborer des stratégies d'atténuation des risques et des stratégies de gestion des risques sur lesquelles on se fondera pour apporter des modifications relativement au confinement physique et aux pratiques opérationnelles dans l'installation concernée.
Exigences opérationnelles	Mesure ou procédure administrative appliquées dans une zone de confinement pour protéger le personnel, l'environnement et, ultimement, la communauté contre les matières infectieuses et les toxines, comme énoncé au chapitre 4 de la Norme canadienne sur la biosécurité.
Exportation	Activité qui consiste à expédier (p. ex. transférer ou transporter) des agents pathogènes, des toxines ou d'autres matières infectieuses réglementées en provenance du Canada vers un autre pays.

Exposition	Contact ou proximité étroite avec des matières infectieuses ou des toxines pouvant respectivement causer une infection ou une intoxication. Les voies d'exposition sont l'inhalation, l'ingestion, l'inoculation et l'absorption.
Groupe de risque (GR)	Groupe dans lequel les matières biologiques sont classées en fonction de leurs caractéristiques inhérentes, comme la pathogénicité, la virulence, le risque de propagation et l'existence d'un traitement prophylactique ou thérapeutique efficace. Le groupe de risque énonce le risque pour la santé du personnel et du public ainsi que la santé des animaux et des populations animales.
Habilitation de sécurité en vertu de la <i>Loi sur les agents pathogènes humains et les toxines</i> (Habilitation de sécurité en vertu de la LAPHT)	Autorisation délivrée par l'Agence de la santé publique du Canada, en vertu de l'article 34 de la <i>Loi sur les agents pathogènes humains et les toxines</i> , à la suite d'une vérification des antécédents et de la cote de fiabilité d'une personne.
Haute direction	Autorité ultimement responsable de la délégation des pouvoirs appropriés en matière de biosécurité. La haute direction est chargée de s'assurer que le programme de biosécurité dispose de ressources suffisantes, que les exigences légales sont respectées, que l'ordre de priorité des problèmes à l'égard de la biosécurité est bien établi et que ces problèmes sont corrigés adéquatement.
Importation	Activité qui consiste à introduire au Canada (p. ex. transfert, transport, manutention) des agents pathogènes, des toxines ou d'autres matières infectieuses réglementées en provenance d'un autre pays.
Incident	Événement ou situation pouvant causer une blessure, du mal, une infection, une intoxication, une maladie ou un dommage. Les incidents peuvent mettre en cause des matières infectieuses, des animaux infectés ou des toxines. Le déversement, la libération et la perte de matières infectieuses ou de toxines ainsi que l'exposition à celles-ci, la fuite d'un animal, les cas où un employé se blesse ou développe une maladie, l'accès non autorisé à la zone de confinement, une panne de courant, un incendie, une explosion, une inondation ainsi que toutes les autres situations de crise (p. ex. séisme, ouragan) sont des exemples d'incidents. Les accidents et ceux évités de justesse sont considérés comme des incidents.
Infection (ou intoxication) contractée en laboratoire (ICL)	Infection ou intoxication dues à une exposition à des matières infectieuses, à des animaux infectés ou à des toxines manipulés ou entreposés dans la zone de confinement.

Installation	Structure, bâtiment ou aire définie à l'intérieur d'une structure ou d'un bâtiment dans lesquels sont manipulées ou entreposées des matières infectieuses ou des toxines. Il peut s'agir d'un laboratoire de recherche, d'un laboratoire de diagnostic, d'une aire de production à grande échelle ou d'une zone où l'on héberge des animaux. Ce terme désigne également une succession de pièces ou un bâtiment contenant plusieurs de ces aires.
Intoxication	Troubles ou maladies causés par une substance qui peuvent être symptomatiques ou asymptomatiques et entraîner un dérèglement physiologique. L'intoxication fait suite à l'exposition (c.-à-d. l'ingestion, l'inhalation, l'inoculation ou l'absorption) d'une toxine produite par un microorganisme ou isolée de celui-ci. Une intoxication peut aussi être provoquée par l'exposition à une toxine microbienne de synthèse.
Inventaire	Liste des ressources biologiques d'une zone de confinement répertoriant les agents pathogènes, les toxines et les matières infectieuses entreposés à l'intérieur comme à l'extérieur de la zone de confinement.
Laboratoire	Installation même ou aire située à l'intérieur d'une installation dans lesquelles on manipule des matières biologiques à des fins scientifiques ou médicales.
Libération	Rejet de matières infectieuses ou de toxines hors du système de confinement.
Maladie	Trouble structural ou fonctionnel touchant un humain ou un animal vivant, ou une partie du corps de ceux-ci. Les maladies sont causées par une infection ou une intoxication et se manifestent généralement par des signes et des symptômes caractéristiques.
Manipulation ou entreposage	Englobent la possession, la manipulation, l'utilisation, la production, l'entreposage, le transfert, l'importation, l'exportation, la libération, le rejet ou l'abandon de toute autre manière infectieuse ou de toxines, ainsi que le fait de permettre l'accès à de telles substances. La manipulation et l'entreposage englobent donc toutes les activités réglementées comportant des agents pathogènes humains ou des toxines énoncées au paragraphe 7(1) de la <i>Loi sur les agents pathogènes humains et les toxines</i> .
Manuel de biosécurité	Manuel propre à une installation dans lequel on décrit les principaux éléments d'un programme de biosécurité (p. ex. plan de biosûreté, formation, équipement de protection individuel).
Matière biologique	Microorganisme pathogène ou non pathogène, protéine ou acides nucléiques, ou toute autre matière biologique pouvant contenir un de ces éléments, en partie ou en entier. Bactéries, virus, champignons, prions, toxines, organismes génétiquement modifiés, acides nucléiques, échantillons de tissus, échantillons de diagnostic, vaccins vivants et isolats d'un agent pathogène (p. ex. les cultures pures, les suspensions, les spores purifiées), tous sont des exemples de microorganismes.

Matière infectieuse	Tout isolat d'un agent pathogène ou toute matière biologique qui contient des agents pathogènes humains ou des agents zoopathogènes et, donc, qui représente un risque pour la santé humaine ou animale.
Menace externe	Personne non autorisée ou qui n'a pas de droit d'accès aux ressources sécurisés, aux zones de confinement ou aux installations. Cette personne peut représenter un risque pour la biosûreté et ne pas être officiellement liée à l'installation.
Menace interne	Personne autorisée à accéder aux ressources sécurisées, aux zones de confinement ou aux installations dans le cadre de son travail. Cette personne peut représenter un risque pour la biosûreté.
Niveau de confinement (NC)	Exigences minimales liées au confinement physique et aux pratiques opérationnelles visant la manipulation sécuritaire de matières infectieuses et de toxines dans les laboratoires, les zones de production à grande échelle et les environnements de travail avec des animaux. Il existe quatre niveaux de confinement, allant du niveau de base (niveau de confinement 1 [NC1]) au niveau le plus élevé (niveau de confinement 4 [NC4]).
Passe-plat	Compartiment à deux portes muni d'un système d'interverrouillage qui traverse une barrière de confinement. Le passe-plat permet d'introduire des matières dans une zone de confinement et de les en retirer en toute sécurité.
Pathogénicité	Capacité d'un agent pathogène de causer une maladie chez un hôte humain ou animal.
Permis	Autorisation délivrée par l'Agence de la santé publique du Canada en vertu de l'article 18 de la <i>Loi sur les agents pathogènes humains et les toxines</i> , permettant de mener une ou plusieurs activités réglementées comportant des agents pathogènes humains ou des toxines.
Personne autorisée	Personne ayant reçu le droit de pénétrer sans supervision dans une zone de confinement par le directeur de cette zone, l'agent de la sécurité biologique ou toute autre personne à laquelle cette responsabilité a été confiée. Pour obtenir ce statut, il faut satisfaire à diverses exigences en matière de formation et faire preuve de compétence envers les procédures opératoires normalisées, selon le jugement des responsables de l'installation.
Plan d'intervention d'urgence (PIU)	Document énonçant les mesures à prendre et les parties responsables en cas d'urgence, par exemple en cas : de déversement, d'exposition, ou de libération de matières infectieuses ou de toxines; de fuite d'un animal; de blessure ou de maladie chez un membre du personnel; de panne de courant; d'incendie; d'explosion; ou de toute autre situation d'urgence (p. ex. inondation, tremblement de terre, ouragan).

Possibilité de double usage	Propriété d'un agent pathogène ou d'une toxine de pouvoir être utilisés autant pour mener des activités scientifiques légitimes (p. ex. à des fins commerciales ou médicales, aux fins de recherche) que pour créer sciemment une arme biologique ayant la capacité de causer une maladie (p. ex. le bioterrorisme).
Procédure opératoire normalisée (PON)	Document qui normalise, en fonction d'une évaluation locale des risques, les procédures et les pratiques de travail sécuritaires utilisées dans le cadre d'activités comportant des matières infectieuses ou des toxines.
Quantité seuil	Quantité minimale au-dessus de laquelle une toxine réglementée en vertu de la <i>Loi sur les agents pathogènes humains et les toxines</i> est qualifiée de « toxine précisée » et, donc, considérée comme un agent biologique à cote de sécurité élevée, comme décrit au paragraphe 10(2) du <i>Règlement sur les agents pathogènes humains et les toxines</i> .
Recherche scientifique	Selon la définition de l'article 1 du <i>Règlement sur les agents pathogènes humains et les toxines</i>, il s'agit d'une enquête ou d'une recherche systématique dans laquelle on étudie un domaine de la science ou de la technologie au moyen d'activités réglementées. Il y a trois types de recherche scientifique : a. la recherche pure, c'est-à-dire lorsque les activités réglementées sont exercées pour faire avancer la science sans qu'il existe d'applications pratiques en vue; b. la recherche appliquée, c'est-à-dire lorsque les activités réglementées sont exercées pour faire avancer la science et qu'il existe une application pratique en vue; c. le développement expérimental, c'est-à-dire lorsque les activités réglementées sont exercées pour réaliser des progrès scientifiques ou technologiques afin de créer de nouveaux produits, matières, procédés ou dispositifs ou d'améliorer ceux qui existent.
Ressources (biologiques)	Tous les agents pathogènes, les matières infectieuses et les toxines en possession d'une installation. D'autres ressources peuvent comprendre du matériel, de l'équipement, des matières non infectieuses, des animaux, des connaissances et de l'information (p. ex. protocoles, données de recherche), et le personnel dans une installation.
Risque	Probabilité qu'un événement indésirable (p. ex. accident, incident, bris de confinement) survienne et conséquences de cet événement.
Salle animalière	Salle conçue pour héberger des animaux dans des cages de confinement primaire. Ces espaces servent seulement pour les petits animaux (p. ex. souris, rats, lapins).
Système de confinement	Équipement réservé à la fonction d'assurer et de maintenir un certain niveau de confinement. Les dispositifs de confinement primaire (p. ex. enceintes de sécurité biologique), les systèmes de chauffage, de ventilation et d'air

	conditionné (CVAC), les systèmes de contrôle et les systèmes de décontamination (p. ex. autoclaves) sont des exemples de systèmes de confinement.
Système de contrôle d'accès	Système physique ou électronique conçu pour ne laisser passer que les personnes autorisées.
Talonnage (passage en double)	Accès sans autorisation à une zone à accès restreint en suivant une personne autorisée à travers le point d'accès, avec ou sans son consentement.
Toxine (microbienne)	Substance toxique produite par un microorganisme, ou dérivée de celui-ci, qui peut avoir des effets graves sur la santé humaine ou animale. Les toxines sont énumérées à l'annexe 1 et à la partie 1 de l'annexe 5 de la <i>Loi sur les agents pathogènes humains et les toxines</i> .
Transfert	Changement de possession (c.-à-d. de propriété) d'agents pathogènes, de toxines ou d'autres matières infectieuses réglementées entre des personnes qui travaillent dans une même installation ou dans des installations différentes (c.-à-d. leur déplacement d'un ou des endroits indiqués sur le permis ou le permis d'importation d'agents zoopathogènes à tout autre endroit).
Transport	Fait de transporter (p. ex. expédition ou acte de transport), au Canada ou à l'étranger, des matières infectieuses ou des toxines vers un bâtiment ou un emplacement différent du sien (c.-à-d. dont l'adresse n'est pas la même), conformément à la Loi de 1992 sur le transport des marchandises dangereuses et au <i>Règlement sur le transport des marchandises dangereuses</i> .
Vulnérabilité	Élément de l'évaluation des risques de biosûreté qui cerne les faiblesses d'une installation relatives aux barrières de sécurité physiques, aux pratiques opérationnelles (p. ex. la formation en matière de biosûreté), à la sécurité du personnel, à la sécurité du transport, à la sécurité de l'information ainsi qu'à la gestion des programmes.
Zone de confinement	Espace physique qui répond aux exigences liées à un niveau de confinement donné. Il peut s'agir d'une salle unique (p. ex. laboratoire de niveau de confinement 2 [NC2]), d'une série de salles situées dans un même endroit (p. ex. plusieurs espaces de travail en laboratoire de NC2 non adjacents, mais verrouillables) ou d'une série de salles adjacentes (p. ex. salles de niveau de confinement 3 [NC3] comprenant des aires réservées au travail en laboratoire et des salles animalières ou des box séparés). La zone de confinement peut comprendre des zones réservées au soutien, notamment des sas équipés de douches, de vestiaires « propres » et de vestiaires « sales », le cas échéant.

RESSOURCES



CHAPITRE 10 - RESSOURCES

10.1 Ressources générales

CEN Workshop 55 – CEN Workshop Agreement (CWA) 16393:2012, *Laboratory biorisk management – Guidelines for the implementation of CWA 15793:2008*. (2012).

Fennelly, L. (2013). *Effective Physical Security* (4th ed.). Waltham, MA, États-Unis : Elsevier Inc.

Centers for Disease Control and Prevention des États-Unis, Division of Select Agents and Toxins et Animal and Plant Health Inspection Service Agriculture Select Agent Program. (2013). *Security Guidance for Select Agent or Toxin Facilities* (2nd Revision). Consulté le 8 février 2016 à l'adresse http://www.selectagents.gov/resources/Security_Guidance_v3-English.pdf

Gendarmerie royale du Canada. (2014). *Sélection de l'équipement de destruction* – section 2. Consulté le 8 février 2016 à l'adresse http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/page_0068_f.htm

Gouvernement du Canada (2012). *Guide de gestion intégrée du risqué: Approche recommandée pour la préparation d'un profil de risque organisationnel*. Consulté le 9 février 2016 à l'adresse <http://www.tbs-sct.gc.ca/hgw-cgf/pol/rm-gr/girm-ggir/girm-ggirtb-fra.asp>

Gouvernement du Canada. (2015). *Norme canadienne sur la biosécurité*, 2^e éd., Ottawa, ON, Canada : Gouvernement du Canada.

Gouvernement du Canada. (2016). *Guide canadien sur la biosécurité*, 2^e éd., Ottawa, ON, Canada : Gouvernement du Canada.

ISO 9001:2008, Systèmes de management de la qualité - Exigences. (2008). Genève, Suisse: Organisation internationale de normalisation.

National Institutes of Health des États-Unis, National Science Advisory Board for Biosecurity. (2011). *Guidance for Enhancing Personnel Reliability and Strengthening the Culture of Responsibility*. Consulté le 8 février 2016 à l'adresse http://osp.od.nih.gov/sites/default/files/resources/CRWG_Report_final.pdf

Salerno, R. M., & J. Gaudioso. (2007). *Laboratory Biosecurity Handbook*. Boca Raton, FL, États-Unis: CRC Press.

Sécurité publique Canada. Centre canadien de réponse aux incidents cybernétiques. Ottawa, ON, Canada : Sécurité publique Canada. Consulté le 8 février 2016 à l'adresse <http://www.securitepublique.gc.ca/cnt/ntnl-scr/cbr-scr/ccirc-ccirc-fr.aspx>

Sécurité publique Canada. (2013). *Guide Pensez cybersécurité pour les petites et moyennes entreprises*. Ottawa, ON, Canada : Sécurité publique Canada. Consulté le 8 février 2016 à l'adresse <http://www.pensezcybersecurite.gc.ca/cnt/rsrscs/pblctns/sml-bsnss-gd/index-fr.aspx>

Sécurité publique Canada. (2016). *Orientation et conseils techniques en matière de cybersécurité*. Consulté le 8 février 2016 à l'adresse <http://www.securitepublique.gc.ca/cnt/ntnl-scrct/cbr-scrct/tchncl-dvc-gdnc-fr.aspx>

Tumpey T, Basler C, Aguilar P, Zeng H, Solórzano A, Swayne D, Cox N, Katz J, Taubenberger J, Palese P, García-Sastre A. (2005). Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus. *Science*, 310(5745):77-80.

United States Geological Survey, United States Department of Interior. (2005). *Physical Security Handbook, 440-2-H*. Consulté le 8 février 2016 à l'adresse <http://www.usgs.gov/usgs-manual/handbook/hb/440-2-h/440-2-h.html>

10.2 Lois du gouvernement du Canada

Loi de 1992 sur le transport des marchandises dangereuses (L.C. 1992, ch. 34). (2015).

Loi sur la santé des animaux (L.C. 1990, ch. 21). (2015).

Loi sur les agents pathogènes humains et les toxines (L.C. 2009, ch. 24). (2015).

Règlement sur la santé des animaux (C.R.C., ch. 296). (2015).

Règlement sur le transport des marchandises dangereuses (DORS/2001-286). (2015).

Règlement sur les agents pathogènes humains et les toxines (DORS/2015-44). (2015).

