Innovation, Science and Economic Development Canada
Innovation, Sciences et Développement économique Canada
Canada

Guide à l'intention des organismes de recherche et de financement sur l'élaboration d'un plan de sécurité de la recherche

La présente publication est disponible en ligne au https://science.gc.ca/site/science/fr/protegez-votre-recherche/lignes-directrices-outils-pour-mise-oeuvre-securite-recherche/guide-lintention-organismes-recherche-financement-lelaboration-dun-plan-securite-recherche.

Pour obtenir un exemplaire de cette publication ou un média substitut (Braille, gros caractères, etc.), veuillez remplir le formulaire de demande de publication au www.ic.gc.ca/demande-publication ou communiquer avec :

Le Centre de services aux citoyens d'ISDE

Innovation, Sciences et Développement économique Canada

Édifice C.D. Howe

235, rue Queen

Ottawa (Ontario) K1A 0H5

Canada

Téléphone (sans frais au Canada) : 1-800-328-6189

Téléphone (international) : 613-954-5031

ATS (pour les personnes malentendantes) : 1-866-694-8389

Heures de bureau : 8 h 30 à 17 h (heure de l'Est)

Courriel : ISED@canada.ca

Autorisation de reproduction

Numéro de catalogue : Iu37-38/2023F-PDF

ISBN 978-0-660-47275-1

N.B. Dans cette publication, la forme masculine désigne tant les femmes que les hommes.

Also available in English under the title *Guidance for Research Organizations and Funders on Developing a Research Security Plan*.

Table des matières

Préface

Les organismes de recherche et de financement[1] jouent un rôle important dans la diversification et le renforcement de l'écosystème de recherche du Canada en menant et en finançant des projets et des partenariats de recherche qui contribuent au bien-être social et économique de notre pays. Le gouvernement du Canada s'est engagé à veiller à ce que ces organismes disposent du soutien et des outils nécessaires pour protéger leurs travaux, ou ceux qu'ils soutiennent, contre l'ingérence étrangère, l'espionnage, le vol et le transfert indésirable de connaissances. Il est important que les organismes de recherche et de financement protègent leurs travaux afin de s'assurer que ceux-ci ne sont pas exploités de manière involontaire ou indésirable. Les répercussions négatives d'une sécurité inadéquate de la recherche peuvent comprendre une diminution de la confiance dans les données et les résultats de la recherche; la perte de données de recherche; la perte de contrôle sur la propriété intellectuelle, les possibilités de brevet et les revenus potentiels; des conséquences juridiques ou administratives; la perte de partenariats futurs potentiels; et une réputation ternie. Les politiques et les pratiques en matière de sécurité de la recherche au Canada visent à empêcher que l'innovation canadienne serve à faire progresser les systèmes d'armes militaires et la technologie de surveillance d'États hostiles. Étant donné que les menaces contre la recherche canadienne évoluent et prennent de nombreuses formes, un effort collectif doit être déployé pour renforcer la résilience du Canada en matière de sécurité de la recherche : les chercheurs, les organismes de recherche, les organismes de financement et les gouvernements partagent tous la responsabilité de déterminer et d'atténuer les risques pour la sécurité nationale liés aux partenariats de recherche.

Le présent guide appuie l'engagement du gouvernement du Canada à l'égard de la sécurité de la recherche, lequel comprend le maintien des principes fondamentaux de la science ouverte et de la liberté universitaire. La science ouverte et la sécurité de la recherche sont complémentaires et se renforcent mutuellement, et cet équilibre est nécessaire pour que la recherche profite au Canada et à tous les Canadiens. Des conseils complémentaires se trouvent dans le portail Protégez votre recherche, y compris les Lignes directrices sur la sécurité nationale pour les partenariats de recherche.

Veuillez noter que le présent document d'orientation est destiné aux organismes de recherche et de financement qui ne sont pas actuellement tenus par le gouvernement du Canada de mettre en œuvre le Formulaire d'évaluation des risques conformément aux Lignes directrices sur la sécurité nationale pour les partenariats de recherche.

[1] Les organismes de financement sont définis comme des organismes qui distribuent des fonds à des bénéficiaires (organisations ou particuliers) qui mènent ou appuient des projets de recherche et des activités connexes, comme la formation en recherche.

1. But

Le présent document a pour but de fournir aux organismes de recherche et de financement des conseils sur la façon d'exercer une diligence raisonnable en matière de sécurité de la recherche en élaborant et en mettant en œuvre un plan de sécurité de la recherche qui établit un processus d'identification, d'évaluation et d'atténuation des risques pour la sécurité nationale avec une approche systémique, cohérente et documentée. Plus précisément, le présent guide aidera les organismes de recherche et de financement à démontrer comment ils peuvent :

- cerner et analyser les risques associés aux types de projets de recherche qu'ils mènent et financent et qui comprennent des partenariats, et déterminer les menaces associées à tout partenaire de recherche concerné; et
- élaborer et mettre en œuvre une série de pratiques exemplaires et de mesures d'atténuation des risques à la sécurité de la recherche adaptées au niveau du projet et de l'organisation, qui soient à la fois réalisables et proportionnelles aux risques.

Bien que le présent document soit axé sur les organismes de recherche et de financement, les principes et les pratiques qui y sont décrits devraient être appliqués et adaptés – au besoin – afin de contribuer à l'élaboration des plans de sécurité des organismes qui soutiennent ou mènent d'autres activités connexes, notamment la formation, le transfert de technologie ou le développement des entreprises.

2. Composantes d'un plan de sécurité de la recherche

2.1 Objectifs du plan de sécurité de la recherche

Le *plan de sécurité de la recherche* d'un organisme de recherche ou de financement devrait appuyer et compléter l'approche globale du gouvernement du Canada en matière de sécurité de la recherche, laquelle se veut compatible avec tous les pays et entreprises. Les sections ci-dessous décrivent les éléments clés d'un *plan de sécurité de la recherche* complet, qui soutient l'intégration des considérations de sécurité nationale dans les pratiques de recherche et de financement. Ces considérations comprennent les suivantes :

- l'évaluation de la sensibilité de la recherche, y compris la question de savoir si la recherche pourrait présenter un risque de vol, d'espionnage ou d'ingérence étrangère ou en être la cible;
- l'évaluation du niveau de risque de toute organisation partenaire impliquée dans la recherche;
- l'évaluation de la posture de sécurité existante de l'organisme de recherche ou de financement; et
- l'élaboration et la mise en œuvre de mesures efficaces d'atténuation des risques pour gérer les risques cernés.

2.2 Connaissez la recherche que vous financez ou menez

Les organismes de recherche et de financement devraient bien comprendre les recherches et les projets qu'ils mènent ou financent, ainsi que leurs applications potentielles respectives (militaires et civiles), afin d'évaluer correctement le niveau de risque pour la sécurité nationale et de déterminer les biens devant être protégés.

Dans le contexte du présent document, la recherche sensible – ainsi que ses données sous-jacentes et les technologies qui en résultent – est définie comme la recherche et les technologies qui pourraient être utilisées pour faire progresser les capacités militaires, de renseignement ou de surveillance d'un État étranger. L'accès non autorisé à la recherche sensible peut nuire aux intérêts du Canada en matière de sécurité nationale ou à ceux de ses pays alliés en ayant une incidence négative sur la capacité du Canada à cerner ces menaces et à y réagir, ou en perturbant l'économie, la société et les infrastructures essentielles du Canada. La recherche sensible comprend la recherche à double usage, c'est-à-dire les produits, les données, les connaissances ou les technologies qui, bien qu'ils soient élaborés ou recueillis à des fins légitimes, peuvent être acquis ou exploités illicitement par autrui pour causer délibérément des préjudices ou encore pour menacer la santé publique ou la sécurité nationale. La recherche sensible comprend également les technologies nouvelles et émergentes dont les applications potentielles dans le domaine militaire, de la sécurité et du renseignement sont moins claires et moins connues, ainsi que les domaines de recherche liés aux minéraux critiques et aux chaînes d'approvisionnement en minéraux critiques; les domaines de recherche qui concernent des données personnelles; ou les domaines de recherche axés sur les infrastructures essentielles.

L'**annexe A** des Lignes directrices sur la sécurité nationale pour les partenariats de recherche dresse la liste des domaines de recherche sensibles que les organismes de sécurité nationale du Canada ont déterminés comme pouvant avoir un double usage ou qui sont ciblés par des gouvernements, des militaires, leurs représentants, ou d'autres acteurs étrangers pour leur potentiel en vue de faire progresser leurs capacités et leurs intérêts en matière de sécurité nationale.

Pour obtenir de plus amples renseignements sur les risques associés à la recherche sensible, veuillez consulter la page Web « Évaluez votre profil de risque » accessible depuis le portail Protégez votre recherche du gouvernement du Canada.

2.3 Connaissez vos partenaires

Les organismes de financement et les organismes de recherche devraient connaître et évaluer les risques associés aux organisations partenaires susceptibles de participer à la recherche qu'ils financent ou mènent. Cela comprend le risque que le partenaire transfère les connaissances, les données ou les résultats de la recherche à un gouvernement étranger, à des militaires, à leurs représentants ou à d'autres acteurs et, ce faisant, nuire aux intérêts du Canada en matière de sécurité nationale.

Les organisations partenaires qui appartiennent à un État ou qui sont soumises à l'influence d'un État pourraient faciliter le transfert non autorisé de connaissances, de technologies ou de propriété intellectuelle à des gouvernements étrangers, à des militaires, à leurs représentants ou à d'autres

acteurs d'une manière qui pourrait nuire à la sécurité nationale du Canada. Ce risque est particulièrement élevé dans le cas d'organisations partenaires associées à des pays dont les lois ou les pratiques obligent les entités et les particuliers à se soumettre aux ordres de leur gouvernement. De telles organisations partenaires manquent d'autonomie et d'indépendance et peuvent recevoir l'ordre de gouvernements étrangers de céder des renseignements, des connaissances de recherche, des technologies ainsi que la propriété intellectuelle y étant associée, qu'ils viennent du Canada ou d'autres pays.

Les risques peuvent également provenir du personnel de l'organisation partenaire qui participe à un projet, surtout si ces personnes ont des liens avec des armées, des institutions ou des gouvernements étrangers étant reconnus pour le transfert non autorisé de connaissances. Leur influence sur les données et les infrastructures (physiques et numériques) et leur accès à celles-ci peuvent servir à favoriser l'accès non désiré aux données ou le transfert de connaissances en dehors du champ d'application du partenariat de recherche.

Consultez l'**Annexe B** des Lignes directrices sur la sécurité nationale pour les partenariats de recherche pour d'autres facteurs qui pourraient entraîner un risque accru de transfert non désiré du savoir à un gouvernement, des militaires, leurs représentants, ou d'autres acteurs étrangers.

Pour obtenir de plus amples renseignements sur la détermination des risques associés aux partenariats de recherche, veuillez consulter la page Web « Quels sont les risques pour la sécurité nationale associés aux partenariats de recherche? » accessible depuis le portail Protégez votre recherche du gouvernement du Canada.

2.4 Connaissez la posture de sécurité de votre organisme

Pour protéger les biens essentiels, y compris les données et les résultats de la recherche, les organismes de recherche et de financement sont encouragés à évaluer de façon proactive leur posture de sécurité existante sur le plan organisationnel. La posture de sécurité d'un organisme désigne l'état de préparation général de l'organisme et la capacité de celui-ci à prévenir, détecter et contrer les menaces ou les attaques. Une bonne pratique consiste à déterminer d'autres domaines de vulnérabilité au sein de l'infrastructure et des processus opérationnels d'un organisme qui pourraient contribuer à un accès non autorisé à ses méthodes, techniques et résultats de recherche. Pour protéger efficacement la recherche et la propriété intellectuelle qui sont détenues ou financées par un organisme de recherche ou de financement, il est avantageux de déterminer et d'évaluer les domaines de risque de l'organisme, notamment :

- **La sécurité physique :** L'adoption de contrôles de sécurité physique appropriés peut réduire le risque d'accès non autorisé à des biens désignés et à d'autres matériels sensibles.
- **La compétence et la fiabilité du personnel** : L'évaluation de la compétence actuelle et continue d'une personne à occuper un poste peut réduire le risque qu'une personne ayant un accès puisse compromettre des biens.
- **La gestion de l'information et la cybersécurité :** La protection de l'information sensible contre l'accès non autorisé ou le vol et l'application du niveau de confidentialité requis peuvent réduire le risque de transfert involontaire de renseignements.

- **L’intervention en cas d’incident et d’urgence :** Signaler et gérer de manière appropriée les événements susceptibles de porter atteinte aux renseignements, au personnel, à la communauté de recherche ou à l’environnement physique de travail peut contribuer à atténuer les incidents et à en réduire l’ampleur lorsqu’ils se produisent, ainsi qu’à réduire le risque de récurrence.

Comprendre les sources des menaces

Les menaces peuvent provenir de particuliers ou de groupes à l’intérieur ou à l’extérieur d’une organisation. Les **menaces internes** peuvent provenir de toute personne ayant connaissance de l’infrastructure et des renseignements d’une organisation, ou y ayant accès, et qui pourrait, par inadvertance ou sciemment, exploiter cet accès à des fins illégitimes ou pour causer des préjudices. Les **menaces externes** englobent les particuliers ou les groupes qui n’ont pas d’accès autorisé aux biens d’une organisation, mais qui agissent d’une manière qui pourrait conduire à l’acquisition illégitime de biens et à des préjudices ultérieurs.

Par exemple, les installations de recherche qui effectuent et conservent leurs travaux sur place peuvent être la cible d’auteurs malveillants qui cherchent à accéder à leurs données, renseignements, connaissances et/ou infrastructures de recherche. Les acteurs malveillants peuvent employer diverses méthodes, notamment la prise de photos de l’installation ou des documents qui s’y trouvent, le vol de renseignements numériques au moyen de dispositifs de stockage portables (p. ex., USB) ou l’accès à des zones à accès restreint en tirant parti de barrières de sécurité physiques inefficaces.

Les données de recherche numériques peuvent également être ciblées par des acteurs malveillants au moyen de rançongiciels, de l’hameçonnage et d’autres cyberattaques qui exploitent les vulnérabilités de l’infrastructure ou des pratiques de cybersécurité afin d’accéder à des données, des renseignements ou des connaissances sur la recherche qui ne seraient pas autrement accessibles au public.

2.5 Déterminer les mesures d’atténuation des risques

Les organismes de financement et les organismes de recherche devraient définir et appliquer des mesures susceptibles de réduire les risques de sécurité cernés afin de protéger la recherche qu’ils financent et ses résultats escomptés. Il s’agit notamment d’établir des mesures d’atténuation des risques au niveau de l’organisme et, au besoin, au niveau du projet. Dans les cas où les risques pour les intérêts canadiens ne peuvent être suffisamment atténués, ou lorsque les risques l’emportent sur les avantages potentiels, ces projets ou partenariats de recherche ne devraient pas être financés ou poursuivis.

Tous les organismes, projets et programmes sont uniques. Certains risques peuvent être suffisamment atténués grâce aux politiques et aux mesures déjà en place, tandis que d’autres peuvent nécessiter des mesures d’atténuation des risques supplémentaires. Au final, l’atténuation des risques devrait être proportionnelle au niveau de risque. Les organismes de recherche devraient se familiariser avec les nombreux types de mesures d’atténuation pratiques qui peuvent être adoptées pour faire face aux risques.

Pour obtenir de plus amples renseignements sur les mesures d'atténuation potentielles pouvant être appliquées aux projets de recherche, veuillez consulter le guide intitulé « Atténuer les risques économiques et géopolitiques associés aux projets de recherche sensibles », accessible depuis le portail Protégez votre recherche du gouvernement du Canada.

3. Cadre de gouvernance de la sécurité de la recherche

Chaque organisme de recherche et de financement sont uniques et mènent ou financent un éventail de programmes de recherche qui présentent des niveaux de risque variables pour la sécurité de la recherche.

Dans le cadre de l'élaboration d'un plan de sécurité de la recherche, les organismes de recherche et de financement devraient procéder à un exercice interne afin de déterminer quels programmes ou projets pourraient être à risque d'ingérence étrangère, de vol et de transfert indésirable des connaissances. Cette analyse préliminaire vient appuyer une approche ciblant les risques qui sert à réduire le fardeau administratif et à concentrer les ressources limitées sur les programmes ou les projets qui présentent un niveau de risque plus élevé.

Bien que l'objectif principal de cet exercice d'établissement de la portée soit de déterminer quels programmes présentent un risque en raison de la participation d'un partenaire potentiellement préoccupant, ce processus peut également relever d'autres domaines de risque (p. ex., les risques liés à la propriété intellectuelle, à l'infrastructure cybernétique et de technologie de l'information ou à l'accès physique) qui contribuent au profil de risque global d'un programme ou d'un projet individuel. Les organismes de recherche et de financement sont encouragés à élaborer un plan de sécurité de la recherche qui soit complet et qui indique clairement les processus, ressources, effectifs ou capacités supplémentaires qui sont nécessaires pour mettre en œuvre efficacement une stratégie réalisable, proportionnée et adaptée.

Au moment d'élaborer leur plan de sécurité de la recherche, les organismes devraient adhérer aux principes de la sécurité de la recherche, y compris, sans toutefois s'y limiter : maintenir un engagement à l'égard de la science ouverte; permettre un haut degré d'adaptabilité dans leurs mesures de sécurité de la recherche; veiller à la reddition de comptes et à la responsabilisation; et s'assurer que les interventions sont proportionnelles aux risques. Toute mesure liée à la sécurité de la recherche devrait continuer à respecter les principes en matière d'intégrité de la recherche, notamment la liberté universitaire, l'autonomie des établissements scolaires, l'équité, la diversité et l'inclusion, ainsi que la transparence.

Pour en savoir plus sur les principes en matière d'intégrité de la recherche et de sécurité de la recherche, veuillez consulter la publication intitulée *G7 Common Values and Principles on Research Security and Research Integrity* (Valeurs communes et principes du G7 en matière de sécurité et d'intégrité de la recherche; en anglais seulement). En intégrant ces principes directeurs dans un plan

de sécurité de la recherche, un organisme de recherche ou de financement peut assurer l'intégrité et la sécurité de la recherche qu'il finance ou mène.

3.1 Élaboration et mise en œuvre du plan de sécurité de la recherche au niveau du projet

Les organismes de recherche et de financement ont des pratiques internes, des politiques, des procédures et des processus d'évaluation du financement qui diffèrent. Par conséquent, le présent document d'orientation vise à tenir compte de ces variations et fournit un cadre flexible pour guider les organismes de recherche et de financement lorsqu'il s'agit de mettre en œuvre des mesures de collecte de renseignements, d'évaluation des risques et d'atténuation de ceux-ci.

Quelle que soit l'approche adoptée par un organisme de recherche ou de financement, le plan de sécurité de la recherche devrait décrire comment l'organisme ou de financement entend atteindre ces objectifs au cours de l'évaluation des projets de recherche.

3.1.1 Déterminer votre approche

L'objectif de tout plan de sécurité de la recherche est de définir un ensemble de politiques et de pratiques courantes devant être employées pour prendre en compte et aborder les risques de manière cohérente pendant la réalisation ou le financement d'une recherche.

Au moment d'élaborer un plan de sécurité de la recherche, il existe des modèles et des ressources de gestion des risques qui peuvent être mis à contribution pour intégrer la sécurité de la recherche dans les processus internes. Notamment, cela inclut le Formulaire d'évaluation des risques selon les Lignes directrices sur la sécurité nationale pour les partenariats de recherche.

Alternativement, les organismes de recherche ou de financement peuvent développer leurs propres outils et processus pour recueillir et évaluer les renseignements sur les risques et déterminer les mesures d'atténuation des risques.

A) Formulaire d'évaluation des risques

Le Formulaire d'évaluation des risques a été élaboré afin d'appuyer la mise en œuvre des Lignes directrices sur la sécurité nationale pour les partenariats de recherche. Celui-ci est conçu pour évaluer les risques que les partenariats de recherche peuvent présenter pour la sécurité nationale et la prospérité économique du Canada. Ce formulaire comprend une série de questions propres aux partenariats de recherche, à la nature de la recherche et à la détermination des mesures d'atténuation.

Les organismes de recherche peuvent utiliser une partie ou la totalité des questions du Formulaire d'évaluation des risques pour évaluer les risques associés aux projets de recherche. Le Formulaire d'évaluation des risques peut être mis à jour périodiquement pour tenir compte de l'évolution des risques pour la sécurité, ainsi que des besoins des chercheurs et des organismes de financement. Pour remplir le Formulaire d'évaluation des risques et y valider les renseignements qui s'y trouvent, il

faut utiliser des méthodes et des outils de recherche basés sur la diligence raisonnable, dont beaucoup sont accessibles auprès de sources ouvertes[2].

B) Méthode autonome

Les organismes de recherche et de financement peuvent également adapter des éléments du Formulaire d'évaluation des risques à leurs fins, ou élaborer leur propre méthode de collecte et d'évaluation des renseignements sur les risques et les mesures d'atténuation associés aux projets de recherche et aux organisations partenaires. La méthode employée devrait s'harmoniser avec les objectifs généraux du gouvernement décrits dans les Lignes directrices sur la sécurité nationale pour les partenariats de recherche. Rappelons que ces objectifs comprennent les suivants :

- l'évaluation de la sensibilité de la recherche, y compris si la recherche pourrait présenter un risque de vol, d'espionnage ou d'ingérence étrangère ou en être la cible;
- l'évaluation du niveau de risque de tout partenaire impliqué dans la recherche; et
- la détermination de mesures efficaces d'atténuation des risques pour gérer les risques cernés.

Les approches, quelles qu'elles soient, devraient également être conçues pour respecter les principes en matière d'intégrité de la recherche, dont la liberté universitaire, l'autonomie institutionnelle, l'équité, la diversité et l'inclusion, ainsi que la transparence, entre autres.

3.1.2 Mise en œuvre de votre plan de sécurité de la recherche

Un plan de sécurité de la recherche devrait énoncer clairement les processus de gouvernance et de prise de décisions prévus par l'organisme pour intégrer la sécurité de la recherche dans ses activités internes. L'organisme de recherche ou de financement devrait préciser clairement quand aura lieu l'intégration de tous les nouveaux processus et toutes les nouvelles structures devant être mis en œuvre. Une telle précision permettra également de déterminer quand et où les ressources devraient être affectées.

Les organismes de recherche et de financement devraient décrire précisément ***comment*** ils comptent mettre en œuvre les aspects suivants de leur cadre de gouvernance de la sécurité de la recherche.

Mener et accroître la sensibilisation aux risques de sécurité de la recherche

Les organismes de recherche et de financement pourraient décrire, par exemple, et s'il y a lieu :

- le mécanisme ou les mesures que l'organisme de recherche ou de financement prévoit utiliser pour sensibiliser davantage l'ensemble de sa communauté aux risques pour la sécurité de la recherche (p. ex., conférence, atelier, documentation sur le programme, séance de sensibilisation, cours en ligne[3], etc.);

[2] Pour en savoir plus sur la diligence raisonnable en matière de sources ouvertes, consultez la publication du gouvernement du Canada intitulée Faire preuve de diligence raisonnable en utilisant des renseignements de sources ouvertes afin de protéger les partenariats de recherche.
[3] De nombreuses ressources sont offertes dans le portail Protégez votre recherche, y compris deux cours rapides en ligne intitulés Introduction à la sécurité de la recherche et Cybersécurité pour les chercheurs.

- qui, au sein de l'organisme de recherche ou de financement, élaborera des initiatives internes de sensibilisation à la sécurité de la recherche et des documents d'information;
- qui, au sein de l'organisme de recherche ou de financement, réalisera toutes les activités de sensibilisation qui ont été élaborées à l'interne;
- quand l'organisme de recherche ou de financement diffusera les documents de sensibilisation;
- comment l'organisme de recherche ou de financement avisera sa communauté des exigences nouvelles ou modifiées en matière de recherche ou de demande de financement.

Recueillir des renseignements auprès des chercheurs ou des demandeurs sur la sensibilité de la recherche, les organisations partenaires et les mesures d'atténuation des risques afférents

Les organismes de recherche et de financement pourraient décrire, par exemple, et s'il y a lieu :

- la fréquence et le moment auxquels l'organisme de recherche ou de financement procédera à des évaluations des risques de sécurité de la recherche;
- la façon dont les renseignements seront recueillis (voir la section 3.1.1 du présent document);
- qui, au sein de l'organisme de recherche ou de financement, sera chargé de recueillir des renseignements sur la recherche, les partenaires et les mesures d'atténuation des risques du demandeur;
- la façon dont l'organisme de recherche ou de financement traitera les renseignements manquants ou les demandes de recherche ou de financement incomplètes (p. ex., si un demandeur indique des risques dans sa demande de partenariat de recherche, mais ne fournit aucun plan d'atténuation).

Évaluer les risques et l'efficacité des mesures d'atténuation

Les organismes de recherche et de financement pourraient décrire, par exemple, et s'il y a lieu :

- la capacité interne existante et l'expertise externe à laquelle l'organisme devra avoir recours, au besoin, pour contribuer à l'évaluation des risques et des mesures d'atténuation;
- qui, au sein de l'organisme de recherche ou de financement, évaluera les éléments de sécurité de la recherche d'une demande (recherche, partenaires, mesures d'atténuation), et qui, au sein de l'organisme, déterminera si des mesures d'atténuation supplémentaires sont justifiées;
- la façon dont l'organisme de recherche ou de financement examinera et mettra à jour périodiquement son approche d'évaluation pour tenir compte de l'évolution et de l'apparition de risques ou de menaces pour la recherche et les projets;
- qui, au sein de l'organisme de recherche ou de financement, formulera une recommandation à l'intention de l'organe décisionnel chargé de l'autorisation ou du financement de demandes ou de projets de recherche;
- le seuil de risque que l'organisme de recherche ou de financement utilisera pour déterminer si une demande présente un niveau de risque inacceptable.

Prendre des décisions

Les organismes de recherche et de financement pourraient décrire, par exemple, et s'il y a lieu :

- qui, au sein de l'organisme de recherche ou de financement, approuvera les décisions de financement (quelle est la structure de responsabilisation interne);

- comment et où l'organisme de recherche ou de financement consignera la justification de chaque décision d'octroi;
- les facteurs ou critères qui seront utilisés pour rendre une décision de financement ou d'autorisation d'un projet;
- la façon dont l'organisme de recherche ou de financement communiquera les décisions de financement aux chercheurs ou demandeurs;
- la façon dont l'organisme de recherche ou de financement traitera les appels relatifs aux décisions de financement.

Maintenir les pratiques de conformité, de surveillance et de production de rapports

Les organismes de recherche et de financement pourraient décrire, par exemple, et s'il y a lieu :

- l'approche en matière de conformité et d'application qui a été adoptée pour responsabiliser les personnes quant au respect du plan de sécurité de la recherche;
- la façon dont l'organisme de recherche ou de financement intégrera les modalités de sécurité de la recherche dans les ententes de subvention existantes et futures;
- la façon dont le plan de sécurité de la recherche de l'organisme de recherche ou de financement sera intégré aux politiques, aux contrats, aux codes de conduite, entre autres, des universités;
- les outils de promotion et de surveillance de la conformité et l'éventail des mesures d'application dont dispose l'organisme de recherche ou de financement;
- la façon dont l'organisme de recherche ou de financement traitera les cas de non-conformité;
- qui, au sein de l'organisme de recherche ou de financement, a le pouvoir de prendre des mesures disciplinaires en cas de non-conformité;
- qui, au sein de l'organisme de recherche ou de financement, est responsable de consigner les incidents et les atteintes à la sécurité;
- la façon dont l'organisme de recherche ou de financement rendra compte du type et du nombre d'incidents ou d'atteintes à la sécurité; et
- qui, au sein de l'organisme de recherche ou de financement, est chargé de répondre aux questions sur la sécurité de la recherche.

3.2 Élaboration et mise en œuvre de votre plan de sécurité de la recherche sur le plan organisationnel.

En plus d'exprimer la façon dont un organisme de recherche ou de financement déterminera, évaluera et atténuera les risques pour la sécurité associés à ses projets et partenariats de recherche, ces organismes ont la responsabilité de protéger les renseignements et la recherche qui sont recueillis auprès des chercheurs et des demandeurs de financement. Un plan de sécurité de la recherche au niveau de l'organisme a pour but de renforcer les activités internes de l'organisme afin de protéger celui-ci contre les menaces à la sécurité de la recherche, tant à l'interne qu'à l'externe.

3.2.1 Mise en œuvre de votre plan de sécurité de la recherche

Cet aspect du plan de sécurité de la recherche doit indiquer clairement comment l'organisme de recherche ou de financement prévoit tenir à jour les facteurs à prendre en compte en matière de sécurité de la recherche, les modifier ou les intégrer à ses stratégies organisationnelles et de gestion des risques.

Les organismes de recherche devraient fournir des renseignements précis sur ***comment*** ils prévoient tenir compte à l'interne des composantes et des aspects suivants en matière de sécurité :

Maintenir la sécurité physique

Les organismes de recherche et de financement pourraient décrire, par exemple, et s'il y a lieu :

- qui surveillera l'apparition de menaces internes et externes susceptibles de mettre en péril l'infrastructure de l'organisme et la résilience de la sécurité de la recherche;
- qui a accès aux zones à accès restreint au sein des installations de recherche;
- les types de visiteurs qui sont ou ne sont pas autorisés à entrer dans le bâtiment physique ou dans le laboratoire de recherche;
- les contrôles de l'accès physique et de l'accès aux données que l'organisme de recherche ou de financement a mis en place, y compris les barrières physiques, la surveillance, les alarmes et les mécanismes de détection des accès non autorisés;
- les mesures de protection mises en place pour l'équipement appartenant à l'organisme de recherche ou de financement;
- les systèmes de secours ou de stockage des données existants;
- la façon dont la recherche et les biens connexes seront protégés lorsque le personnel voyage à l'étranger.

Assurer la compétence et à la fiabilité du personnel

Les organismes de recherche et de financement pourraient décrire, par exemple, et s'il y a lieu :

- les protocoles d'enquête de sécurité préalables à l'embauche du personnel ainsi que les procédures continues de vérification de la compétence et de la fiabilité;
- qui effectuera les vérifications des références et de sécurité appropriés;
- la façon dont les conflits d'intérêts potentiels ou existants du personnel seront relevés et abordés;
- les exigences de formation du personnel en matière de sécurité qui sont en place ou qui seraient élaborées.

Intégrer les pratiques de gestion de l'information et de cybersécurité[4]

Les organismes de recherche et de financement pourraient décrire, par exemple, et s'il y a lieu :

- la façon dont l'organisme de recherche ou de financement classifiera chaque bien et en déterminera le niveau de sécurité;
- la méthode de stockage des données personnelles, de la recherche et des renseignements recueillis auprès des chercheurs et des demandeurs;
- qui a accès à la propriété intellectuelle, à la recherche, aux données personnelles et à tout autre renseignement sensible;
- les mécanismes en place pour assurer la sécurité du stockage de la propriété intellectuelle, de la recherche et des données personnelles;
- la façon dont les éventuelles lacunes de cybersécurité seront relevées et évaluées[5];
- la façon dont l'organisme de recherche ou de financement partagera ou publiera ses données, ses méthodes de recherche, ses résultats, entre autres, avec les demandeurs et les partenaires respectifs; et
- les politiques mises en place au sein de l'organisme de recherche ou de financement pour veiller au transfert sécuritaire des connaissances et de la recherche aux intervenants concernés.

Adopter des mesures d'intervention en cas d'incident et d'urgence[6]

Les organismes de recherche et de financement pourraient décrire, par exemple, et s'il y a lieu :

- les mécanismes mis en place pour détecter les accès non autorisés aux installations, à la propriété intellectuelle, à la recherche et aux données personnelles (c.-à-d. détecter les atteintes à la sécurité physique, les cyberincidents, la perte éventuelle de propriété intellectuelle; les conflits d'intérêts, etc.);
- la façon dont les incidents seront signalés à l'interne et à l'externe, et à qui;
- la façon dont les incidents seront traités en temps opportun et de manière coordonnée; et
- les procédures d'enquête sur les incidents mises en place.

[4] Les plans de sécurité de la recherche peuvent être reliés au plan de cybersécurité d'un organisme, s'il existe, ou y faire référence. Une autre solution possible pourrait être d'intégrer volontairement le plan de cybersécurité à un plan de sécurité de la recherche.

[5] Pour en savoir plus sur les pratiques et les facteurs à prendre en compte en matière de cybersécurité, veuillez consulter la « Série de cours d'apprentissage en ligne CyberSécuritaire Canada », des cours virtuels offerts par le gouvernement du Canada.

[6] Un plan d'intervention en cas d'incident et d'urgence est un ensemble de procédures permettant de réagir rapidement et efficacement à des situations susceptibles d'avoir une incidence sur la sécurité des biens et des personnes. Il devrait comprendre des procédures de signalement des incidents, d'intervention en cas d'incident et d'enquête sur les incidents.

4. Dernières réflexions

En résumé, le principal objectif d'un *plan de sécurité de la recherche* est d'établir un cadre de gouvernance démontrant comment les organismes de recherche et de financement entendent déterminer et évaluer la recherche qui pourrait présenter un risque de vol, d'espionnage ou d'ingérence étrangère ou en être la cible, et élaborer et mettre en œuvre des mesures d'atténuation qui soient à la fois réalisables et proportionnelles aux risques.

L'élaboration et la mise en œuvre d'un plan de sécurité de la recherche renforceront le cadre de sécurité existant d'un organisme et faciliteront la réalisation des objectifs qui protègent la recherche canadienne et les intérêts du Canada en matière de sécurité nationale. En outre, l'utilisation d'un plan de sécurité de la recherche permettra aux organismes de recherche et de financement de maintenir un niveau élevé de transparence entre les chercheurs, les demandeurs de financement, les partenaires et le gouvernement.

Bref, un plan de sécurité de la recherche est un mécanisme que les organismes de recherche et de financement peuvent utiliser pour renforcer la culture de la sécurité de la recherche au sein de leur organisme et pour sensibiliser leur communauté à l'importance de la sécurité de la recherche. Au final, un plan de sécurité de la recherche devrait démontrer l'engagement et la responsabilité partagée d'un organisme de recherche ou de financement à l'égard de la protection de l'écosystème de recherche du Canada par des mesures proportionnelles aux risques, l'amélioration continue et l'intégration de la sécurité de la recherche dans ses processus opérationnels.