Mitacs

# Plan de sécurité de la recherche

# PLAN DE SÉCURITÉ DE LA RECHERCHE MITACS — dernière mise à jour le 12 avril 2023

## 1. Objectifs

Les grands objectifs du Plan de sécurité de la recherche Mitacs sont les suivants :

1. Veiller à ce que les propositions de collaboration de recherche, particulièrement celles comportant la conception de propriété intellectuelle et des mandats avec des partenaires ou des collaborateurs internationaux, présentent suffisamment d'avantages pour le Canada pour pouvoir être admissibles à un financement de Mitacs.

2. Prévenir les violations de la sécurité de la recherche, les actes illicites et les menaces à la sécurité nationale impliquant des gouvernements, des individus et des organisations internationales, comme :
   - le vol de recherche, de données sensibles ou de propriété intellectuelle;
   - l'accès indésiré à de la recherche ou des données sensibles, l'espionnage;
   - les violations de règlements ou de lois du gouvernement canadien (p. ex., les lois sur l'importation et l'exportation), des sanctions.

## 2. Modifications apportées aux demandes présentées à Mitacs ainsi qu'au processus d'évaluation pour améliorer la sécurité de la recherche

Les mises à jour des processus de dépôt de demande et d'évaluation de Mitacs décrites dans cette section ne s'appliquent qu'aux programmes Accélération et Élévation, car ces programmes représentent plus de 70 % de l'activité de Mitacs et impliquent par défaut des organisations partenaires hors du milieu de l'enseignement postsecondaire.

Les autres programmes Mitacs, comme Globalink, Stage de stratégie d'entreprise (SSE) et Mitacs Entrepreneur International (MEI), sont axés sur des collaborations de recherche universitaire ou des activités non liées à la recherche et seront donc analysés lors des prochaines mises à jour du Plan de sécurité de la recherche Mitacs en 2023.

Le processus pour assurer la sécurité de la recherche comporte trois étapes, décrites dans les trois sous-sections 2.1-2.3 ci-dessous.

### 2.1 Identification des collaborations internationales et évaluation des avantages pour le Canada

Mitacs demandera à toutes les personnes qui présentent une demande de répondre à trois questions permettant de déterminer si leur proposition comporte un aspect de collaboration internationale.

La recherche impliquera-t-elle :

- une organisation partenaire qui est située à l'extérieur du Canada ?
- une organisation partenaire qui est une filiale canadienne ou une succursale d'une organisation dont le siège social se trouve à l'extérieur du Canada ?

- un·e professeur·e superviseur·e, un·e stagiaire ou un collaborateur ou une collaboratrice d'une organisation (établissement d'enseignement, entreprise, gouvernement, organisme sans but lucratif) située à l'extérieur du Canada ?

Les personnes qui répondent oui à l'une de ces questions devront remplir le Formulaire de collaboration internationale (voir l'Annexe B du modèle de proposition Accélération), et y fournir des renseignements au sujet des ententes concernant la propriété intellectuelle (PI) découlant de la collaboration proposée. Mitacs évaluera ensuite les avantages de la PI pour le Canada résultant des activités et des accords proposés afin d'éclairer la décision de financement.

Les avantages de la PI pour le Canada seront soupesés au même titre que d'autres avantages tels que la formation de personnel hautement qualifié (PHQ) canadien. Les propositions, qui sont évaluées au cas par cas, doivent démontrer qu'elles généreront suffisamment d'avantages pour le Canada pour pouvoir être financées.

Le cadre d'évaluation des avantages pour le Canada est basé sur le système initialement créé pour les participant·es du programme Accélération International de Mitacs. Ce cadre a été mis en œuvre par Mitacs en 2019 (voir la section sous Mitacs Accélération International ici) et il sera désormais appliqué à toutes les propositions Accélération et Élévation comportant une composante de collaboration internationale.

Tout renseignement personnel recueilli est assujetti à la législation relative à la protection des renseignements personnels et à la Politique de protection des renseignements personnels de Mitacs pour les participantes et participants aux programmes. Pour une description de l'engagement de Mitacs à protéger les renseignements personnels fournis par les demandeurs aux programmes, veuillez consulter https://www.mitacs.ca/fr/declaration-de-confidentialite.

## 2.2 Identification et atténuation des risques de sécurité de la recherche

Mitacs demandera à toutes les personnes déposant une demande de remplir trois déclarations relatives aux risques de sécurité de la recherche.

La recherche impliquera-t-elle :

- l'accès à des installations ou des infrastructures qui entreposent ou transfèrent des données sensibles (p. ex., des données personnelles sensibles ou de grands volumes de données pouvant devenir sensibles en tant qu'ensemble de données compilées) ?
- de la recherche liée à des minéraux critiques, des infrastructures essentielles ou à des domaines de recherche sensibles (voir la description dans l'Annexe A des Lignes directrices sur la sécurité nationale pour les partenariats de recherche)?
- des domaines répertoriés dans la Liste des substances d'exportation contrôlée, la Liste des marchandises d'importation contrôlée, la Liste des pays visés ou des biens/technologies identifiés dans la Liste des marchandises contrôlées ?

Les personnes qui répondent oui à l'un des points énumérés ci-dessus doivent tenir compte des risques pour la sécurité de la recherche liés à la nature des activités proposées. Elles doivent également consulter les politiques, les lignes directrices et les exigences de leur(s) établissement(s) d'enseignement postsecondaire

canadien(s) participant(s) afin de déterminer les mesures appropriées d'atténuation des risques liés à la sécurité de la recherche en fonction des lignes directrices et des énoncés de politique des gouvernements fédéral, territoriaux et provinciaux, et d'identifier toute mesure nécessaire pour assurer le respect des règlements et des lois des gouvernements applicables (p. ex., les lois sur l'importation et l'exportation).

Dans certains cas, Mitacs peut exiger qu'on lui remette des documents confirmant que l'établissement des personnes faisant une demande a bel et bien reçu et approuvé les mesures d'atténuation des risques liés à la sécurité de la recherche pour les activités proposées. Par exemple, Mitacs peut exiger la remise de ces documents comme condition de financement, surtout si la recherche proposée porte sur l'une des priorités du gouvernement, comme les technologies quantiques, l'intelligence artificielle et certains domaines des sciences de la vie, ou encore si la recherche proposée touche à des données ou des matériaux sensibles susceptibles d'intéresser des organisations gouvernementales ou militaires internationales. Ces propositions sont traitées au cas par cas.

### 2.3 Vérification des organisations partenaires

Mitacs procèdera à la vérification des organisations partenaires mentionnées dans toutes les demandes pour :

- interdire à toute organisation partenaire qui est une société prête-nom contrôlée par une entité internationale (p. ex., les entreprises qui n'ont pas d'activités commerciales, d'actifs, de personnel ou de produits/services importants au Canada) de participer aux programmes de Mitacs;
- interdire à toute organisation partenaire dont le nom figure dans les sanctions canadiennes ou qui est située dans un pays faisant partie de la Liste des pays visés de participer aux programmes de Mitacs;
- interdire à toute organisation partenaire signalée par l'une des agences de sécurité canadiennes comme constituant une menace à la sécurité nationale du Canada de participer aux programmes de Mitacs.

## 3. Communications externes

Nous informerons les personnes présentant une demande et les participant·es que Mitacs se réserve le droit :

- de refuser de financer un projet proposé ou en cours à tout moment pour des raisons de sécurité de la recherche;
- d'octroyer un financement conditionnel à la satisfaction d'autres exigences de sécurité, le cas échéant.

Les personnes qui déposent une demande et celles participant au programme seront dirigées vers des ressources gouvernementales sur la sécurité de la recherche (lesquelles peuvent être mises à jour de temps à autre), y compris :

- Gouvernement du Canada — Protégez votre recherche
- Gouvernement du Canada — Comment puis-je évaluer les risques dans le cadre de partenariats ?

Le contenu de la page de renvoi sur la sécurité de la recherche est mis à jour régulièrement pour refléter le Plan de la sécurité de la recherche le plus récent.

## 4. Atténuation des risques liés à la sécurité de la recherche en entreprise

### 4.1 Ressources dédiées

Mitacs affectera un équivalent temps plein au sein de son service de recherche pour soutenir la mise en œuvre du Plan de sécurité de la recherche Mitacs. Cette personne-ressource s'occupera de l'opérationnalisation du processus indiqué aux sections 2.1-2.3, de la coordination de la formation interne du personnel de Mitacs, de la mise à jour des communications externes concernant la sécurité de la recherche, si besoin est, et de la surveillance des risques émergents. Le niveau de ressources nécessaires pour mener à bien ces tâches sera surveillé et évalué régulièrement.

### 4.2 Formation

Mitacs offrira en tout temps une formation à jour sur la sécurité de la recherche à son personnel afin d'assurer une connaissance fondamentale des énoncés de politique et des directives du gouvernement et pour mieux faire connaître les risques de sécurité de la recherche.

### 4.3 Réponse aux risques et menaces émergentes

Mitacs assure une veille de l'actualité et des développements relatifs à l'écosystème de la recherche canadienne pour détecter les signes de risques émergents liés à la sécurité de la recherche. À cette fin, Mitacs garde ouvertes les voies de communication avec les parties prenantes gouvernementales et favorise l'échange de connaissances avec d'autres organismes de recherches, dont les trois organismes subventionnaires fédéraux. De plus, Mitacs dispose d'un plan de cybersécurité pour améliorer la protection de ses renseignements et de ses ressources essentielles au cas où il deviendrait la cible de cyberattaques et de menaces extérieures.