ArcticNet

ᐅᑭᐅᖅᑕᖅᑐᒥᒃ ᑐᑭᓯᓂᐊᖅᑎᑎᑦ

Politique sur la sécurité de la recherche externe pour les bénéficiaires finaux

1. But

La Politique sur la sécurité de la recherche externe d'ArcticNet (la « politique ») a pour but de régir et d'appuyer les activités menées par ArcticNet pour assurer la sécurité de la recherche réalisée dans le cadre de ses programmes de financement destinés aux bénéficiaires finaux.

2. Objectif

La présente politique définit les responsabilités des bénéficiaires finaux concernant la sécurité de la recherche.

3. Approbation et pouvoir

Le conseil d'administration d'ArcticNet a le pouvoir d'approuver la présente politique, ainsi que toute correction ou modification pouvant y être apportée. Deux fois par année, il procèdera à l'examen de la présente politique.

La directrice générale (ou le président-directeur général ou la présidente-directrice générale) d'ArcticNet est responsable de l'opérationnalisation de la présente politique.

4. Définitions

« Entente de financement avec le bénéficiaire final » désigne une entente conclue entre ArcticNet et un bénéficiaire final concernant l'octroi de fonds par ArcticNet aux fins de la réalisation d'un projet admissible.

« Fournisseur de services » désigne une tierce partie avec qui un bénéficiaire final ou l'un des participants à un projet a conclu une entente touchant la prestation des services nécessaires à la réalisation des activités liées au projet, y compris l'aménagement des installations et des infrastructures connexes.

« Incident de sécurité de la recherche » fait référence à tout événement qui compromet la confidentialité, l'intégrité ou la disponibilité des données de recherche, dont l'accès non autorisé, l'atteinte à la sécurité des données ou la perte de documents de recherche.

« Projet admissible » désigne tout projet qu'un bénéficiaire final entreprend afin de réaliser les objectifs d'ArcticNet en vertu de l'entente de financement conclue entre les deux parties.

« Recherche sensible » désigne la recherche à double usage, soit 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. Y sont également inclus 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 et les domaines de recherche axés sur les infrastructures essentielles.

« Sécurité de la recherche » fait référence à l'ensemble des mesures qui sont prises pour protéger l'intégrité de la recherche à l'échelle nationale et internationale en mettant l'accent, en particulier, sur la protection contre les menaces à la sécurité nationale et économique.

« Utilisateur final » désigne un organisme de l'un ou l'autre des types suivants sélectionné par ArcticNet pour recevoir des fonds afin de réaliser des projets admissibles :

- établissements d'enseignement postsecondaire;
- secteur privé;
- établissements canadiens d'enseignement postsecondaire;
- organismes et gouvernements autochtones;
- réseaux de recherche;
- hôpitaux de recherche;
- municipalités;
- réseaux de mobilisation du public;
- organismes sans but lucratif.

5. Engagement

ArcticNet s'engage à favoriser la création d'un environnement de recherche sécuritaire et exige que les bénéficiaires finaux exercent une diligence raisonnable en matière de sécurité de la recherche par la mise en œuvre de mesures de sécurité de la recherche visant à protéger les activités et données de recherche.

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 de cerner ces menaces et d'y réagir, ou en perturbant l'économie, la société et les infrastructures essentielles du Canada. L'annexe A des *Lignes directrices sur la sécurité nationale pour les partenariats de recherche* porte sur les domaines de recherche sensibles qui, selon les organismes de sécurité nationale du Canada, peuvent avoir un double usage ou qui sont ciblés par des gouvernements, des militaires, leurs représentants, ou d'autres acteurs étrangers pour leur potentiel à faire progresser leurs capacités et leurs intérêts en matière de sécurité nationale.

ArcticNet exige que les bénéficiaires finaux s'engagent à élaborer un plan de sécurité de la recherche.

ArcticNet exige également que les bénéficiaires finaux respectent les lois applicables et les autres textes et autorités ayant force exécutoire, tels que les normes, les accréditations et les ordres professionnels, ainsi que les politiques et les procédures d'ArcticNet. En outre, ArcticNet exige qu'ils respectent la Politique des trois organismes sur la gestion des données de recherche, le *Guide à l'intention des organismes de recherche et de financement sur l'élaboration d'un plan de sécurité de la recherche*, ainsi que les *Lignes directrices sur la sécurité nationale pour les partenariats de recherche*.

6. Exigences relatives à la sécurité de la recherche

La section suivante décrit les attentes et les exigences d'ArcticNet à l'égard des bénéficiaires finaux en ce qui concerne la sécurité de la recherche.

7. Cybersécurité

ArcticNet exige que les bénéficiaires finaux veillent à ce que leurs mesures de sécurité de la recherche soient conformes aux politiques et processus de leur établissement ou organisation en matière de cybersécurité, ainsi qu'à toutes les exigences qu'ArcticNet pourrait établir en matière de cybersécurité.

8. Gestion des données

ArcticNet exige que les bénéficiaires finaux élaborent des plans de gestion des données et en assurent la mise à jour. Pour obtenir de plus amples renseignements sur cette exigence, veuillez consulter la Politique de gestion des données d'ArcticNet.

ArcticNet exige également que les bénéficiaires finaux qui utilisent des données produites dans le cadre de projets de recherche réalisés par et avec des collectivités, des collectifs et des organismes des Premières Nations, des Inuits et des Métis veillent à ce que ces données soient gérées conformément aux principes établis et approuvés par ces collectivités, collectifs et organismes, ainsi qu'en partenariat avec ceux-ci.

9. Évaluation

ArcticNet s'engage à examiner les mesures prises par les bénéficiaires finaux concernant la sécurité de la recherche, afin de s'assurer qu'elles répondent aux exigences énoncées dans la présente politique. Dès la présentation d'une demande de financement, les bénéficiaires finaux qui comptent entreprendre un projet visant à faire progresser un domaine de recherche en technologies sensibles doivent remplir le formulaire *Attestation relative à la recherche visant à faire progresser les domaines de recherche en technologies sensibles* remis par ArcticNet à chacun des membres de l'équipe. En outre, si le projet prévoit la participation de partenaires du secteur privé ou d'autres partenaires répondant à la définition ci-dessous de la Fondation canadienne pour l'innovation, les bénéficiaires finaux doivent remplir le Formulaire d'évaluation des risques et le Formulaire d'identification d'un partenaire du secteur privé.

Un partenaire du secteur privé :

- joue un rôle actif dans les activités de recherche décrites dans la proposition (p. ex. partage de la propriété intellectuelle, apport d'expertise, participation active aux activités de recherche, apport financier aux activités de recherche);
- héberge toute l'infrastructure de recherche ou une partie de celle-ci;
- contribue à hauteur de plus de 500 000 $ au coût d'un seul article d'infrastructure, que ce soit en espèces ou en nature.

ArcticNet examinera toutes les demandes présentées dans le cadre des appels de propositions afin de s'assurer qu'elles s'accompagnent du formulaire *Attestation relative à la recherche visant à faire progresser les domaines de recherche en technologies sensibles*, du Formulaire d'évaluation des risques et d'autres documents requis. Si ArcticNet estime que le projet présente un risque moyen ou élevé, il demandera au bénéficiaire final d'élaborer des mesures d'atténuation des risques et collaborera avec l'organisme de soutien à la recherche auquel le bénéficiaire final est

associé afin de répondre aux questions qui pourraient subsister. Les mesures prises par les bénéficiaires finaux concernant la sécurité de la recherche visant à faire progresser un domaine de recherche en technologies sensibles devront faire l'objet d'un examen, et les bénéficiaires finaux devront présenter des rapports d'étape annuels à ArcticNet.

Propriété intellectuelle
Toute la propriété intellectuelle issue des données, y compris les données anonymisées, les ensembles de données, les données étiquetées, les représentations, les modèles entraînés et les résultats, est considérée comme une propriété intellectuelle du projet admissible et assujettie aux engagements et aux exigences de la politique d'ArcticNet sur la propriété intellectuelle.

10. Lieu d'hébergement et protection des données

Les bénéficiaires finaux doivent s'assurer que leurs données et celles de tous les participants à leur projet sont hébergées sur des serveurs situés au Canada. Ils doivent aussi mettre en place des mesures de sécurité techniques et organisationnelles appropriées pour protéger les données contre la perte, l'utilisation, la divulgation, l'altération ou l'accès non autorisés, et se conformer à toute mesure de sécurité pouvant être établie par leur établissement ou organisation et par ArcticNet.

Si les bénéficiaires finaux et les participants à leur projet retiennent les services d'un fournisseur de services pour l'hébergement de leurs données, celles-ci doivent toujours être hébergées sur des serveurs et dans des installations au Canada, détenus, contrôlés et exploités par le fournisseur de services. Les bénéficiaires finaux et les participants à leur projet doivent déployer des efforts raisonnables pour s'assurer que le fournisseur de services est soumis à des contrôles de sécurité de l'information fortement semblables à ceux que requiert l'entente conclue avec le bénéficiaire final.

11. Surveillance

Les bénéficiaires finaux sont tenus de veiller à ce que les risques pour la sécurité de la recherche, les évaluations et les mesures d'atténuation fassent l'objet d'un suivi et d'une surveillance continus, conformément aux politiques et procédures de leur établissement ou organisation sur la sécurité de la recherche, ainsi qu'aux exigences de la présente politique.

12. Production de rapports

ArcticNet exige que les bénéficiaires finaux lui rendent compte rapidement de tout changement apporté à l'étendue de la recherche ou aux partenariats affiliés qui pourrait avoir une incidence sur les niveaux de risque pour la sécurité de la recherche, ainsi que sur les mesures d'atténuation prévues.

13. Incident de sécurité de la recherche

Dès qu'ils prennent connaissance d'un incident de sécurité de la recherche, les bénéficiaires finaux et les participants à leur projet en informent ArcticNet dans les plus brefs délais et au plus tard dans les vingt-quatre heures. Cette notification comprendra au minimum une description de ce qui suit :

- la nature de l'incident, y compris le type de données visées;

- les conséquences probables de l'incident;
- les mesures prises ou proposées par les bénéficiaires finaux et les participants à leur projet pour remédier à la situation, y compris, le cas échéant, les mesures visant à atténuer les éventuels effets négatifs.

Dès qu'ArcticNet est informé d'un incident de sécurité de la recherche, il en informe ses bailleurs de fonds.

Dans l'éventualité où ces renseignements ne seraient pas disponibles au moment de la notification à ArcticNet dudit incident de sécurité de la recherche, les bénéficiaires finaux et les participants à leur projet devront assurer un suivi auprès d'ArcticNet à mesure que les renseignements seront disponibles, afin que l'ensemble des renseignements relatifs à l'incident de sécurité de la recherche soient communiqués dans les plus brefs délais. Les bénéficiaires finaux et les participants à leur projet documenteront les mesures prises à la suite de l'incident de sécurité de la recherche et procèderont à un examen des événements et des mesures prises à la suite de l'incident. La documentation ainsi élaborée sera alors communiquée à ArcticNet.

14. Gestion de la sécurité de la recherche

La section suivante décrit les attentes et les exigences d'ArcticNet à l'égard des bénéficiaires finaux en ce qui concerne la gestion de la sécurité de la recherche :

Connaître son projet
Les bénéficiaires finaux sont tenus de consulter la liste des domaines de recherche en technologies sensibles du gouvernement du Canada afin de déterminer si leur proposition comporte des travaux de recherche visant à faire progresser au moins l'un de ces domaines. Si tel est le cas, ils doivent remplir un formulaire d'attestation et le transmettre à ArcticNet. En remplissant ce formulaire, ils déclarent ne pas être affiliés à l'une des organisations de recherche nommées par le gouvernement du Canada et ne pas recevoir de financement ou de contributions de l'une d'elles.

Connaître les partenaires de son projet
Les bénéficiaires finaux sont tenus d'évaluer les risques associés à la participation de partenaires du secteur privé à leurs projets, afin de déterminer si le projet compte un partenaire du secteur privé qui joue un rôle actif dans le projet ou y contribue en espèces ou en nature. Si un partenaire du secteur privé participe au projet, les bénéficiaires finaux doivent divulguer les établissements affiliés à ce partenaire et élaborer un plan complet d'atténuation des risques possibles pour la sécurité de la recherche. À cette fin, ils doivent remplir le Formulaire d'atténuation des risques et le transmettre à ArcticNet.

Connaître les établissements de recherche auxquels son équipe de recherche est affiliée
Les bénéficiaires finaux doivent divulguer à ArcticNet les établissements de recherche auxquels tous les membres de leurs équipes de recherche sont affiliés. ArcticNet s'assurera ensuite que ces établissements ne figurent pas sur la liste des organisations de recherche nommées.

15. Non-conformité

La non-conformité à la présente politique peut mener à des sanctions, y compris la suspension ou l'arrêt des versements prévus. ArcticNet se réserve le droit de prendre toutes les mesures nécessaires pour en assurer la conformité.

16. Coordonnées

Modification : Le conseil d'administration peut modifier la présente politique.	Dernier examen :
Date d'approbation : Non approuvée étant donné qu'il s'agit d'une politique opérationnelle, mais le conseil d'administration a approuvé la présente version. 11 mars 2025	Dernière révision :