CANADA FOUNDATION FOR INNOVATION

Research security considerations for MSI facilities

February 6, 2025

INNOVATION

Canada Foundation for Innovation

Fondation canadienne pour l’innovation

Research security

CFI's current approach

Currently, our approach to research security is meant to mitigate two types of risks:

- Risks related to partnerships with the **private sector** (in line with the Government of Canada's National Security Guidelines for Research Partnerships (NSGRP))

- Risks related to **affiliations of concern** for projects aiming to advance a sensitive technology research area (as per the Government of Canada's Policy on Sensitive Technology Research and Affiliations of Concern (STRAC policy))

Research security

NSGRP requirements

Currently applies to:	**Not in scope:**
Innovation Fund (2023 & beyond) Northern Fund CBRF – BRIF Stage 2 Exceptional Opportunities Fund Unaffiliated JELF (as of June 25, 2024)	College Fund Affiliated JELF **Major Science Initiatives Fund**

The CFI requires a **Risk Assessment Form (RAF)** and a **Private-sector partner identification form (PSPID)** if the project involves a **private-sector partner** (or partners) that:

- Has an **active role in the research activities described in the proposal** (e.g., sharing of intellectual property, providing expertise, actively participating in research activities, contributing financially to the research activities); or
- **Houses part or all of the research infrastructure**; or
- Contributes **more than $500,000** to the infrastructure through a cash or in-kind contribution to any single item.

Research security

STRAC requirements

Currently applies to:	Not in scope:
Innovation Fund (2025 & beyond) Northern Fund & Exceptional Opportunities Fund Unaffiliated JELF	College Fund Affiliated JELF **Major Science Initiatives Fund**

Project/team leaders and team members will be required to complete an attestation form if the proposal is in support of research that **aims to advance** any of the **areas listed** in the Government of Canada's list of Sensitive Technology Research Areas.

Proposals that support research that aims to advance a sensitive technology research area **will not be funded** if any of **the project/team leaders or team members** are currently affiliated with, or in receipt of funding or in-kind support from, any of the Government of Canada's Named Research Organizations.

Research security

Research infrastructure specifics

We are having preliminary discussions with facilities, but also with the community at large.

Focus on infrastructure-specific risks:

- Risks associated with procurement of infrastructure
  - Research security considerations related to suppliers
- Risks associated with **un**authorized access to infrastructure
  - Cyberattacks, physical security, etc.
- Risks associated with authorized access to infrastructure
  - Affiliations of external and internal users working on projects aiming to advance a sensitive technology research area
  - Level of access of external and internal users

Risks associated with authorized access to infrastructure

- CFI's current approach to STRAC is limited to **team/project leaders** and **team members** identified in proposals for projects where research activities described in the proposal **aim to advance a sensitive technology research area.**
- Currently, our approach does not systematically address risks associated with other users of the infrastructure. Given the number of external users of large facilities such as yours, this is an area that warrants further discussion.

Risks associated with authorized access to infrastructure

Questions:

- Do you currently have processes in place to mitigate risks associated with external and internal users accessing the infrastructure?

- Do you collect information on external users? What and when? What are the challenges related to interacting with external users and gathering information from them?

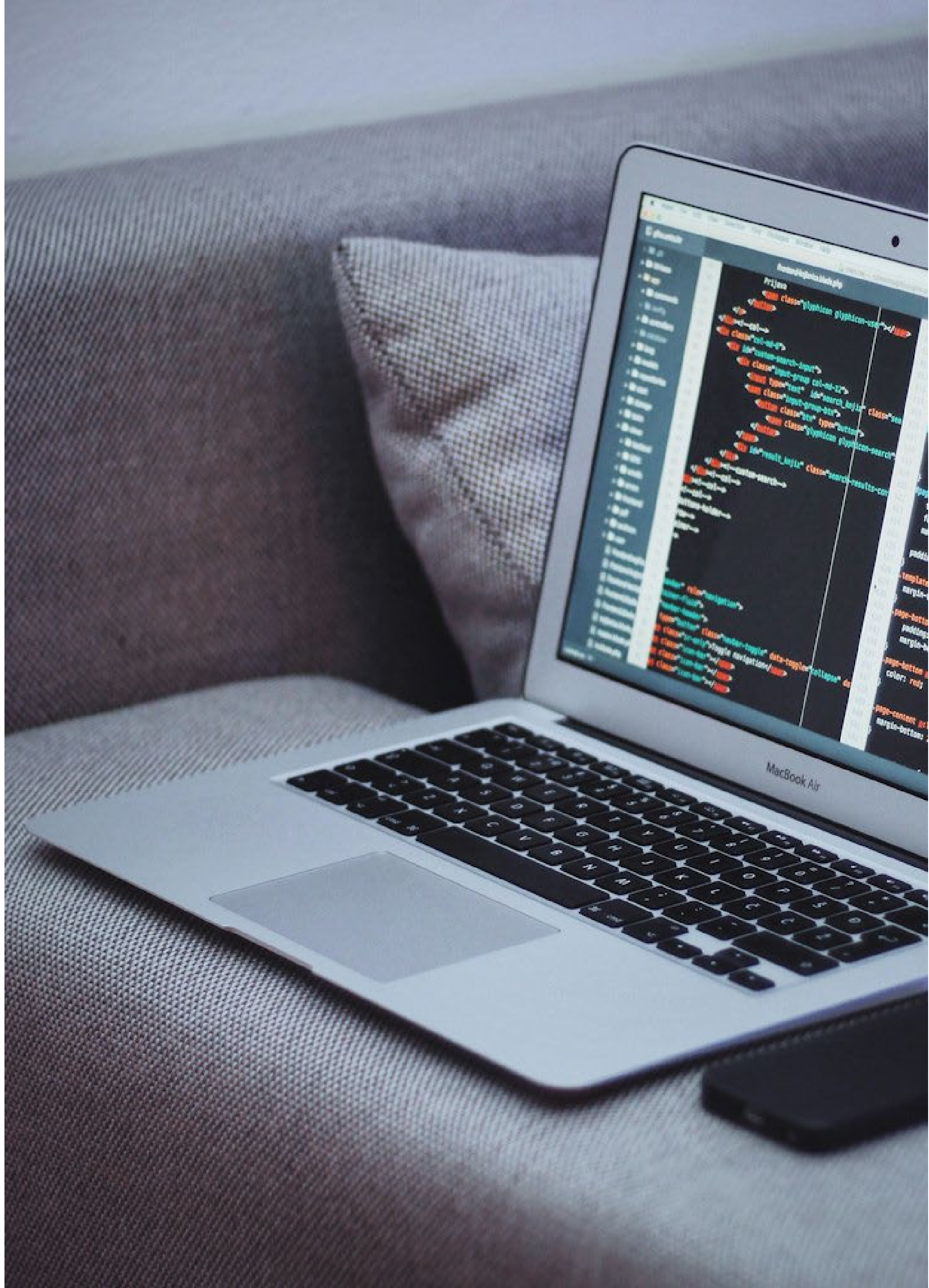
- How different is the interaction with external users depending on whether they access the facility directly or use some sort of “valet service” (e.g., they might send samples to a facility for facility staff to analyze)? Does that change the way you gather information.

Research Security

Want to know more?

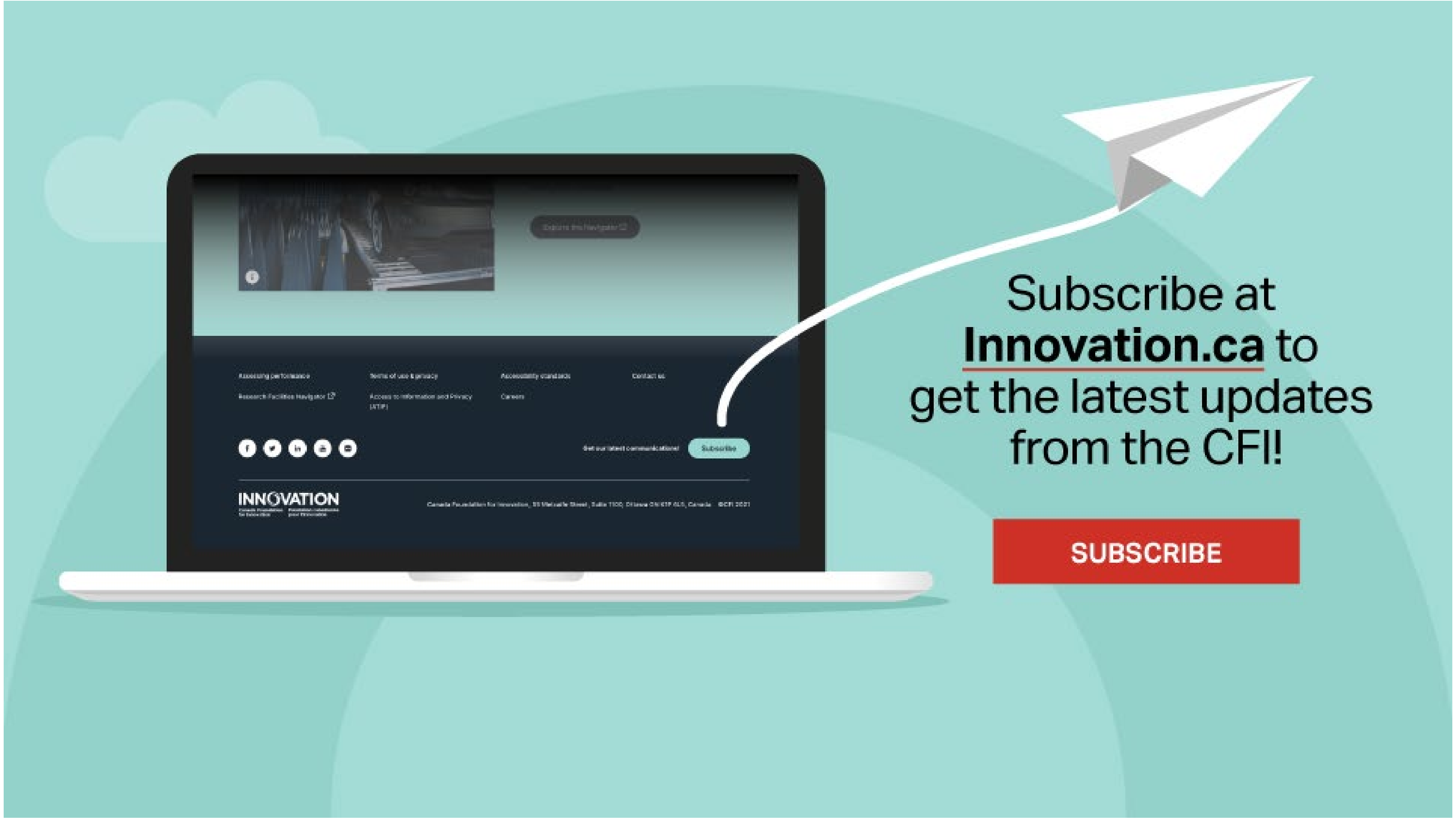
Consult our research security web page or

email us at research.security@innovation.ca.



Thank you

Questions?


Explore the Navigator
Assessing performance
Research Facilities Navigator
Terms of use & privacy
Access to Information and Privacy (ATIP)
Accessibility standards
Careers
Contact us
Get our latest communications!
Subscribe
INNOVATION
Canada Foundation for Innovation
Fondation canadienne pour l'innovation
Canada Foundation for Innovation, 55 Metcalfe Street, Suite 1100, Ottawa ON K1P 6L5, Canada ©CFI 2021

Subscribe at **Innovation.ca** to get the latest updates from the CFI!

SUBSCRIBE

Risks associated with unauthorized access to infrastructure

Questions:

- Do you have specific policies related to physical access and cybersecurity? Are you leveraging those of your institutions?

- Would there be any challenges in implementing such policies at the facility’s level?

Risks associated with procurement of infrastructure

We recognize that malicious actors may use goods and services necessary for carrying out research projects as a vector for theft or unauthorized transfer of data or knowledge.

We also acknowledge that procurement processes are complex and governed by several policies, legislation and trade agreements.

Questions:

- Are sensitivity assessments, aimed at determining the level of the security risk associated with a particular purchase, performed prior to starting the procurement process?

- Do you incorporate clauses related to security in your procurement process? If yes, does it vary with the perceived risk of a particular purchase?

Research security

NSGRP requirements

Institutional responsibility:

Institutions applying for or receiving CFI funding have research security obligations throughout the life of the project. They are required to do the following:

- **At application:** Perform open-source due diligence before submitting an RAF or PSPID (if required).
- **When finalizing:** Implement the risk mitigation plan described in the RAF.
- **Until the final financial report is submitted:** Immediately inform the CFI of changes that could affect the risk to national security (e.g., new partnership with the private sector, change of location of research infrastructure to a private-sector partner).

The CFI’s responsibility:

The CFI and our stakeholders have the responsibility to ensure that Canada’s research ecosystem is safe and secure. We will:

- Assess and validate RAF
- Refer forms to the Government of Canada if:
    - The nature of the proposed research is deemed sensitive; and,
    - Partners are associated with or originating from organizations or countries that are subject to sanctions or associated with criminal and ethical concerns.

Research security

STRAC requirements

The CFI context:

Funding of **large infrastructure projects** complexifies the interpretation of the STRAC policy:

- Are all users of the research infrastructure covered by the policy?
- What about infrastructure located in core facilities with hundreds/thousands of users?
- Which research projects are “in scope”?

Given these questions, our current implementation plan is based on:

- Meeting the imperative of the policy
- Recognizing the resources available.

Our interpretation and next steps:

Currently, in the context of **CFI-funded research infrastructure projects**:

- Only project/team leaders and team members are subject to requirements under the STRAC policy
- While we encourage institutions to take adequate security measures, no other users of the research infrastructure are subject to requirements under the STRAC policy.

We will be initiating a discussion in the coming months with institutions and national security agencies to refine the scope of this implementation.

Research security

STRAC requirements

Institutional responsibility:

Institutions applying for or receiving CFI funding have research security obligations throughout the life of the project.

- **When developing a proposal:** Determine if the research it supports aims to advance any of the sensitive technology research areas.
- **At application:** If it does, all team/project leaders and team members (those providing CVs/biosketches) will need to provide an attestation for the institution to be able to submit the proposal.

  Note: Institutions are not expected to validate the accuracy of attestation forms submitted to the CFI.
- **Until the final financial report is submitted:** Inform the CFI of any changes in project/team leaders (as per usual) and provide a new attestation if required. Inform the CFI immediately of any changes in the nature of the research activities that would result in the project now being aimed at advancing a sensitive technology research area.

Research security

Cybersecurity

Most of the requirements related to cybersecurity involves secure data storage and monitoring, data access, data retention and disposal, and, in general, data management.

In some cases, such as but not limited to core facilities or infrastructure connected to a larger network, the sole presence of the infrastructure require cybersecurity measures.

In this context, we are interested in gathering information about which institutional cybersecurity policies currently apply to such equipment.

Research security

Physical security

CFI funding is mostly dedicated to the acquisition of infrastructure. There are several risks related to the physical security of research infrastructure. As such, it is imperative to maintain all infrastructure safe and secure.

In this context, we are interested in gathering information about institutional policies and processes to ensure the physical security of CFI funded infrastructure.

Research security

Personnel

While most of CFI investments are directed to the acquisition of infrastructure, a portion of its funding goes towards personnel to perform diverse tasks related to the infrastructure.

In this context, we are interested in gathering information about institutional policies and processes for the personnel in receipt of CFI funding.

FONDATION CANADIENNE POUR L'INNOVATION

Facteurs à considérer à propos de la sécurité de la recherche des installations financées par le FISM

6 Février 2025

INNOVATION

Fondation canadienne pour l'innovation

Canada Foundation for Innovation

Sécurité de la recherche

Quelle est l’approche de la FCI en matière de sécurité de la recherche?

Présentement, l’approche de la FCI en matière de sécurité de la recherche consiste à atténuer deux types de risques :

- Les risques liés aux partenariats avec le **secteur privé** (conformément aux Lignes directrices sur la sécurité nationale pour les partenariats de recherche du gouvernement du Canada);
- Les risques liés aux affiliations préoccupantes pour des projets visant à faire progresser un domaine de recherche en technologies sensibles (conformément à la Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes du gouvernement du Canada).

Sécurité de la recherche

Exigences en matière de *risques liés aux partenariats avec le secteur privé*

S'applique présentement aux programmes de financement ci-dessous	**Ne s'applique pas**
Fonds d'innovation (2023 et après) Fonds du Nord Étape 2 du FRBC – FIRSB Fonds des occasions exceptionnelles Fonds des leaders John-R.-Evans – Volet non-affilié (à partir du 25 juin 2024)	Fonds des collèges Fonds des leaders John-R.-Evans – Volet Partenariats **Fonds des initiatives scientifiques majeures**

La FCI a besoin qu'un **Formulaire d'évaluation des risques** et un **Formulaire d'identification d'un partenaire du secteur privé** soient remplis si le projet implique un (ou plusieurs) **partenaire**(s) **du secteur privé**(s) qui:

- **Joue un rôle actif dans les activités de recherche décrites dans la proposition** (par exemple, 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 plus de **500 000 dollars** au coût d'un seul article d'infrastructure, que ce soit en espèces ou en nature.

Sécurité de la recherche

Exigences en matière de *risques liés aux affiliations préoccupantes*

S'applique présentement aux programmes de financement ci-dessous	Ne s’applique pas pour l’instant
Fonds d'innovation (2025 et après) Fonds du Nord et Fonds des occasions exceptionnelles Fonds des leaders John-R.-Evans – Volet non-affilié	Fonds des collèges Fonds des leaders John-R.-Evans – Volet Partenariats **Fonds des initiatives scientifiques majeures**

Chaque responsable d’équipe ou de projet et les membres de l’équipe nommés dans la proposition devront remplir un formulaire d'attestation dans le cas où leur proposition comprendrait des travaux de recherche **visant à faire progresser au moins un domaine de recherche en technologies sensibles** de la liste du gouvernement du Canada.

Une proposition visant à faire progresser un domaine de recherche en technologies sensibles **ne sera pas financée** si un **responsable d’équipe ou de projet, ou un membre de l’équipe**, se trouve affilié à l’une des organisations de recherche nommées par le gouvernement du Canada ou reçoit du financement ou des contributions en nature de l’une d’elles au moment de demander du financement.

Sécurité de la recherche

Infrastructure de recherche

Il s’agit d’une discussion préliminaire avec vous, mais aussi avec la communauté en entier.

Accent sur les risques liés à l’infrastructure:

- Risques associés au processus d’approvisionnement
  - Considération des risques associés aux fournisseurs
- Risques associés à un accès **non** autorisé à l’infrastructure
  - Cyberattaques, sécurité physique
- Risques associés à un accès autorisé à l’infrastructure
  - Affiliation des personnes internes et externes à l’organisation qui utilisent l’infrastructure et dont les projets visent à faire progresser un domaine de recherche en technologies sensibles
  - Niveau d’accès de ceux-ci

Risques associés à un accès autorisé à l’infrastructure

- L’approche de la FCI en lien avec la politique RTSAP se limite aux **responsables d’équipe ou de projet** ainsi qu’aux membres de l’équipe lorsque la recherche soutenue par l’infrastructure **vise à faire progresser un domaine de technologie en recherche sensible**.
- En ce moment, notre approche ne tient pas systématiquement en compte les risques associés aux autres personnes qui utilisent ou bénéficie de l’infrastructure. Puisque vos installations comptent un grand nombre de ces utilisatrices et utilisateurs, une discussion plus approfondie est de mise.

Risques associés à un accès autorisé à l’infrastructure

Questions:

- Avez-vous en place des processus ou des mesures visant à atténuer le risque associé aux personnes internes et externes à l’organisation qui ont accès à vos infrastructures?

- Recueillez-vous de l’information à propos des utilisatrices et utilisateurs externes? Si oui, laquelle et quand la recueillez-vous? Quels sont les défis auxquels vous faites face en leur demandant de l’information?

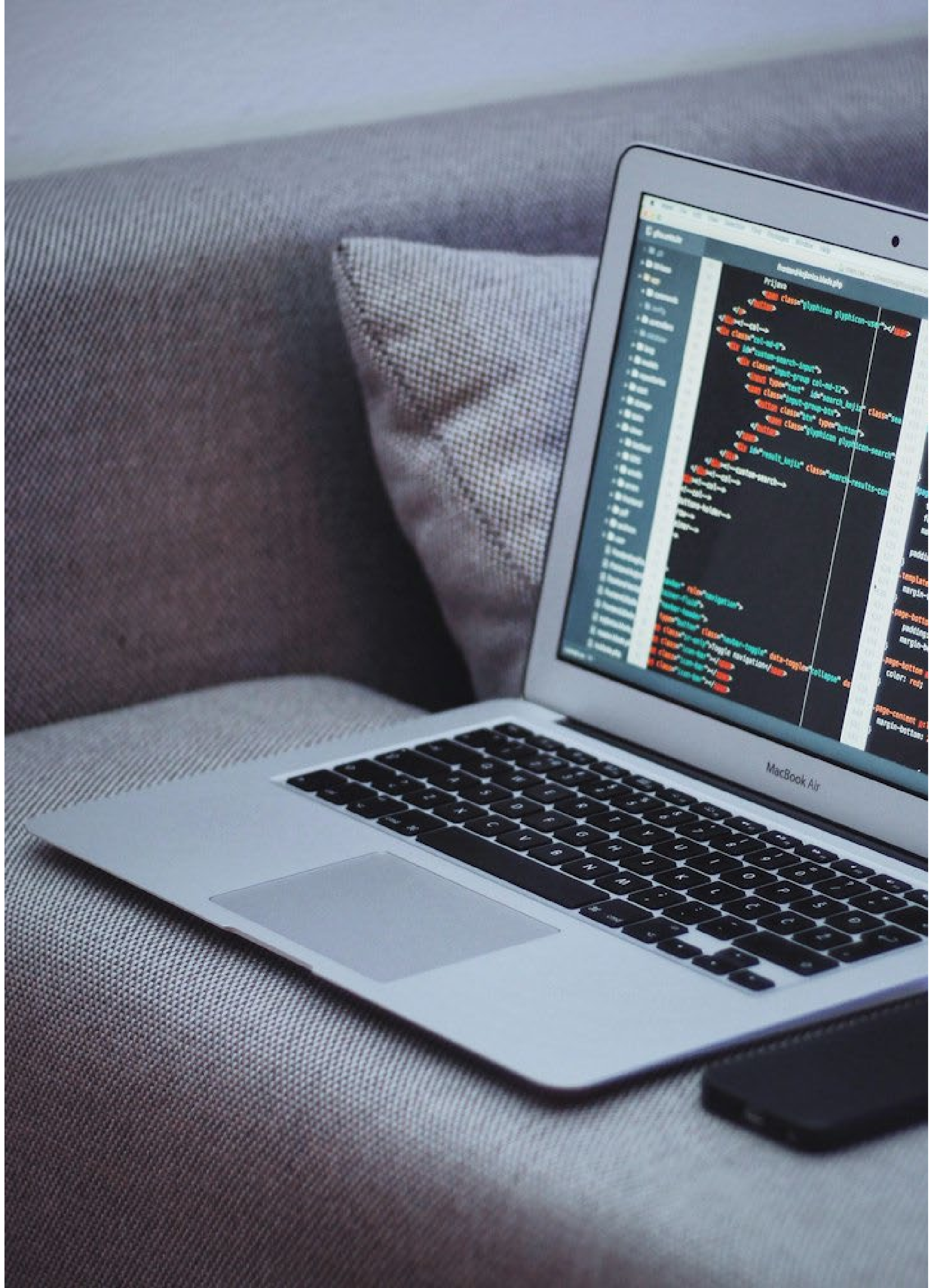
- L’interaction avec les personnes qui utilisent l’infrastructure est-elle différente si ceux-ci ont un accès direct à l’infrastructure ou un a accès par un service de type « valet » (p. ex. en envoyant des échantillons qui sont analysés par le personnel de l’installation)? Cela influence-t-il la façon dont vous recueillez l’information?

Sécurité de la recherche

Vous voulez en savor plus?

Consultez notre site web:
https://www.innovation.ca/fr/appel-gestion/ressources-lien-avec-appels-propositions-gestion-financement/securite-recherche

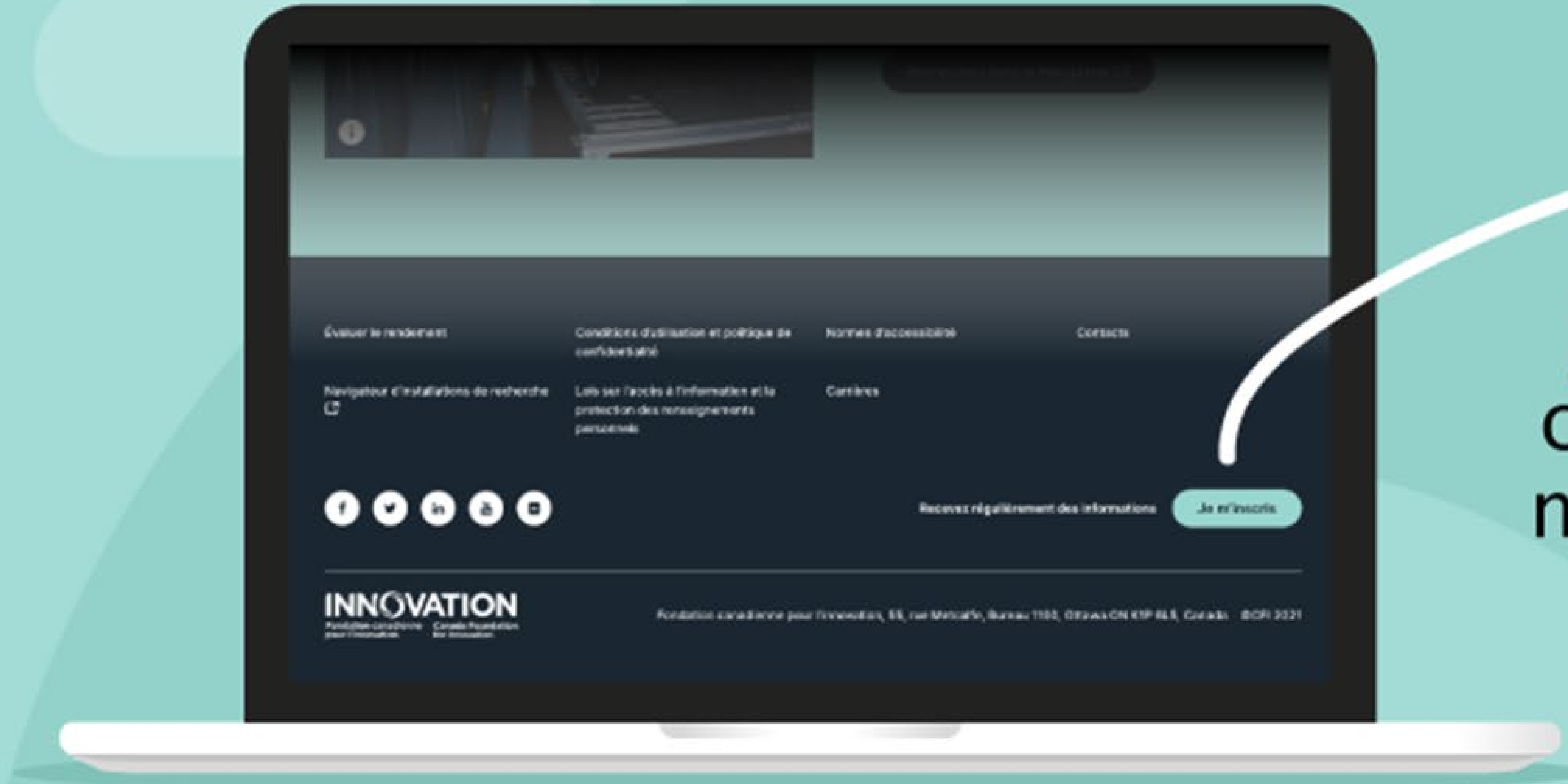
Contactez-nous au
securite.recherche@innovation.ca



CANADA FOUNDATION FOR INNOVATION

Merci

Questions?


Évaluer le rendement
Conditions d'utilisation et politique de confidentialité
Normes d'accessibilité
Contacts
Navigateur d'installations de recherche
Lois sur l'accès à l'information et la protection des renseignements personnels
Carrières
Recevez régulièrement des informations
Je m'inscris
INNOVATION
Fondation canadienne pour l'innovation
Canada Foundation for Innovation
Fondation canadienne pour l'innovation, 55, rue Metcalfe, Bureau 1100, Ottawa ON K1P 6L5, Canada ©CFI 2021

Abonnez-vous à **innovation.ca** pour obtenir les dernières mises à jour de la FCI!

S'ABONNER

Risques associés à un accès non-autorisé à l'infrastructure

Questions:

- Avez-vous des mesures spécifiques liées à la sécurité physique des lieux et à la cybersécurité qui s'appliquent à l'infrastructure? Tirez-vous parti de celles mises en place par votre établissement hôte?

- Anticipez-vous des défis à implanter de telles mesures dans vos installations?

Risques associés au procesus d’approvisionnement

Nous savons que des acteurs malveillants peuvent utiliser les biens et services dont vous avez besoin comme une porte d’entrée pour voler ou transfert de façon non autorisé de données ou de connaissances.

Nous reconnaissons que l’approvisionnement est un processus complexe régi par différentes politiques, législations et accords commerciaux.

Questions:

- Avant de débuter le processus d’approvisionnement en soi, faites-vous une évaluation de la sensibilité de l’acquisition afin de déterminer le niveau de risque en lien avec la sécurité lié à cette acquisition?

- Incluez-vous des clauses en lien avec la sécurité dans vos appels d’offres? Si oui, varient-elles avec le risque perçu de chaque acquisition?

Research security

NSGRP requirements

Institutional responsibility:

Institutions applying for or receiving CFI funding have research security obligations throughout the life of the project. They are required to do the following:

- **At application:** Perform open-source due diligence before submitting an RAF or PSPID (if required).
- **When finalizing:** Implement the risk mitigation plan described in the RAF.
- **Until the final financial report is submitted:** Immediately inform the CFI of changes that could affect the risk to national security (e.g., new partnership with the private sector, change of location of research infrastructure to a private-sector partner).

The CFI's responsibility:

The CFI and our stakeholders have the responsibility to ensure that Canada's research ecosystem is safe and secure. We will:

- Assess and validate RAF
- Refer forms to the Government of Canada if:
  - The nature of the proposed research is deemed sensitive; and,
  - Partners are associated with or originating from organizations or countries that are subject to sanctions or associated with criminal and ethical concerns.

Research security

STRAC requirements

The CFI context:

Funding of **large infrastructure projects** complexifies the interpretation of the STRAC policy:

- Are all users of the research infrastructure covered by the policy?
- What about infrastructure located in core facilities with hundreds/thousands of users?
- Which research projects are “in scope”?

Given these questions, our current implementation plan is based on:

- Meeting the imperative of the policy
- Recognizing the resources available.

Our interpretation and next steps:

Currently, in the context of **CFI-funded research infrastructure projects**:

- Only project/team leaders and team members are subject to requirements under the STRAC policy
- While we encourage institutions to take adequate security measures, no other users of the research infrastructure are subject to requirements under the STRAC policy.

We will be initiating a discussion in the coming months with institutions and national security agencies to refine the scope of this implementation.

Research security

STRAC requirements

Institutional responsibility:

Institutions applying for or receiving CFI funding have research security obligations throughout the life of the project.

- **When developing a proposal:** Determine if the research it supports aims to advance any of the sensitive technology research areas.
- **At application:** If it does, all team/project leaders and team members (those providing CVs/biosketches) will need to provide an attestation for the institution to be able to submit the proposal.

  Note: Institutions are not expected to validate the accuracy of attestation forms submitted to the CFI.

- **Until the final financial report is submitted:** Inform the CFI of any changes in project/team leaders (as per usual) and provide a new attestation if required. Inform the CFI immediately of any changes in the nature of the research activities that would result in the project now being aimed at advancing a sensitive technology research area.

Research security

Cybersecurity

Most of the requirements related to cybersecurity involves secure data storage and monitoring, data access, data retention and disposal, and, in general, data management.

In some cases, such as but not limited to core facilities or infrastructure connected to a larger network, the sole presence of the infrastructure require cybersecurity measures.

In this context, we are interested in gathering information about which institutional cybersecurity policies currently apply to such equipment.

Research security

Physical security

CFI funding is mostly dedicated to the acquisition of infrastructure. There are several risks related to the physical security of research infrastructure. As such, it is imperative to maintain all infrastructure safe and secure.

In this context, we are interested in gathering information about institutional policies and processes to ensure the physical security of CFI funded infrastructure.

Research security

Personnel

While most of CFI investments are directed to the acquisition of infrastructure, a portion of its funding goes towards personnel to perform diverse tasks related to the infrastructure.

In this context, we are interested in gathering information about institutional policies and processes for the personnel in receipt of CFI funding.