Mitacs

Research security plan

MITACS RESEARCH SECURITY PLAN — last updated April 12, 2023

1. Goals

The overarching goals of this Mitacs Research Security Plan are as follows:

1. To ensure that proposals for research collaborations, especially those involving intellectual property development and assignments with foreign partners or collaborators, demonstrate adequate benefits to Canada to qualify for Mitacs funding.

2. To prevent research security breaches, legal violations, and national security threats involving foreign governments, individuals, and organizations, such as:
   - Theft of research, sensitive data, or intellectual property
   - Unwanted access to research or sensitive data, espionage
   - Violation of relevant Canadian government regulations, legislation (e.g., import/export laws), or sanctions

2. Research security enhancements to Mitacs application and review processes

The updates to the Mitacs application and review processes described in this section apply only to the Accelerate and Elevate programs, as these programs account for over 70% of Mitacs activity and inherently involve non-academic partner organizations.

Other Mitacs programs, such as Globalink, Business Strategy Internship (BSI), and Mitacs Entrepreneur International (MEI), focus on academic research collaborations or non-research activities and will be addressed in future updates to the Mitacs Research Security Plan in 2023.

The research security process involves three steps, which are described in the following three subsections 2.1-2.3.

2.1 Identifying international collaborations and assessing benefits to Canada

Mitacs will require all applicants to complete three declarations that identify whether the proposal involves an aspect of international collaboration.

Will the research involve:

- A partner organization located outside Canada?
- A partner organization that is a Canadian subsidiary or branch office of an organization headquartered outside Canada?
- An academic supervisor, intern, and/or collaborator from an organization (academic, industrial, government, or non-profit) located outside Canada?

If yes to any of these items, Mitacs will require applicants to complete an International Collaboration Form (see Appendix B of the Accelerate proposal template). Within this form, Mitacs will require applicants to provide information regarding the intellectual property (IP) arrangement for the proposed collaboration.

Mitacs will then assess the IP benefits to Canada resulting from the proposed activities and agreements to inform the funding decision.

IP benefits to Canada will be considered along with other benefits such as the training of Canadian highly qualified personnel (HQP), and proposals must demonstrate sufficient total benefits to Canada to be funded. Proposals are evaluated on a case-by-case basis.

The framework for assessing benefits to Canada is based on the system first created for participants in Mitacs's Accelerate International program. This framework was implemented by Mitacs in 2019 (see the section under Mitacs Accelerate International on this page) and will now be applied to all Accelerate and Elevate proposals with an international collaboration component.

All personal information collected is subject to privacy legislation and Mitacs Privacy Policy for Program Participants. For a description of Mitacs's commitment to protecting the personal information provided by program applicants, please see http://www.mitacs.ca/en/privacy-policy.

2.2 Identifying potential research security risks and risk mitigation

Mitacs will require all applicants to complete three declarations related to research security risks.

Will the research involve:

- Access to facilities or infrastructure that house or transfer sensitive data (i.e., sensitive personal data or large amounts of data that could be sensitive in the aggregate)?
- Research related to critical minerals, critical infrastructure, or sensitive research areas as discussed in Annex A of the National Security Guidelines for Research Partnership?
- Areas covered by the Export Control List, the Import Control List, the Area Control List, and/or goods/technology identified in the Controlled Goods List?

If yes to any of the items listed above, applicants should consider any potential research security risks associated with the nature of the proposed activities. Applicants should also consult the policies, guidelines, and requirements of their participating Canadian academic institution(s) to determine any appropriate research security risk mitigation measures based on federal and provincial government guidelines/policy statements, and to identify any necessary actions to ensure compliance with relevant government regulations and legislation (e.g., import/export laws).

In certain cases, Mitacs may require applicants to provide documentation to confirm that their institution has received and approved any research security risk mitigation measures for the proposed activities. For example, Mitacs may require such documentation to be submitted as a condition for funding, especially if the proposed research falls under government priorities such as quantum technologies, artificial intelligence, and certain areas of life sciences, or if the proposed research involves sensitive data or materials that may be of interest to foreign government or military organizations. Such proposals are handled on a case-by-case basis.

2.3 Screening partner organizations

Mitacs will screen the partner organizations on all applications to ensure that:

- Any partner organization that is a shell corporation controlled by a foreign entity (for instance, companies lacking significant business operations, assets, employees, product/service offerings within Canada) will not be allowed to participate in Mitacs programs
- Any partner organization listed under Canadian sanctions or based in a country on the Area Control List will not be allowed to participate in Mitacs Programs
- Any partner organization identified by Canadian security agencies as posing a threat to Canadian national security will not be allowed to participate in Mitacs programs

3. External communications

Applicants and program participants will be informed that Mitacs reserves the right to:

- Decline, at any point, funding towards a proposed or ongoing project on the grounds of research security concerns
- Award funding conditional on additional security requirements as appropriate

Applicants and program participants will be directed to government resources on research security which may be updated from time to time, including:

- Government of Canada—Safeguarding Your Research
- Government of Canada—How can I assess risks in partnerships?

Mitacs will continually update the content featured on its landing page on research security to reflect the most up-to-date Mitacs Research Security Plan.

4. Corporate research security risk mitigation

4.1 Dedicated resources

Mitacs will dedicate one full-time equivalent based within its Research department to support the implementation of this Mitacs Research Security Plan. This resource supports the operationalization of the process outlined in sections 2.1-2.3, the coordination of internal training for Mitacs staff, the updates to external communications regarding research security as needed, and the monitoring of emerging risks. The appropriate level of resourcing necessary for carrying out these tasks will be continually monitored and evaluated.

4.2 Training

Mitacs will maintain an ongoing and continually updated research security training program for all staff to ensure a fundamental knowledge of government policy statements and guidelines, and general awareness of research security risks.

4.3 Response to emerging risks and threats

Mitacs monitors current events and developments in the Canadian research ecosystem for signs of emerging risks related to research security. This involves continuing communications with our government stakeholders, as well as appropriate knowledge-sharing with other research organizations including the three federal granting agencies. In addition, the Mitacs Cybersecurity Plan is in place to improve protection of information and critical resources should Mitacs itself become the target of cyber-attacks and external threats.