

MITACS RESEARCH SECURITY PLAN — last updated August 8th, 2024

1. Goals

The overarching goals of this Mitacs Research Security Plan are:

- 1.1 To ensure alignment with the intent of the [National Security Guidelines for Research Partnerships](#) and the [Policy on Sensitive Technology Research and Affiliations of Concern](#).
- 1.2 To ensure that proposals for research collaborations, especially those involving intellectual property (IP) development and/or assignments to non-academic host organizations, demonstrate adequate benefits to Canada to qualify for Mitacs funding.

2. Research security enhancements to Mitacs application and review processes

2.1 Identifying sensitive research areas and affiliations of concern

For all applications to Mitacs programs, applicants must complete the following declaration.

- a) Does the project aim to advance any of the listed [Sensitive Technology Research Areas \(STRAs\)](#)?

Each proposed academic supervisor and intern must also complete the following declaration.

- Are you currently affiliated with, or in receipt of funding or in-kind support, from any of the listed [Named Research Organizations \(NROs\)](#)?

Any applicant who is currently affiliated with, or in receipt of funding or in-kind support from one or more of the institutions on the list of [NROs](#) is not eligible to participate in a Mitacs-funded project involving research that aims to advance a STRA. Mitacs will also screen a sample of applications, selected at its sole discretion, and validate the accuracy of the completed declarations.

Mitacs reserves the right to decline funding, at any point, for a project that advances a sensitive technology research area because of affiliations of concern.

2.2 Assessing research security risks and benefits to Canada

For any application that involves non-academic host organization(s), applicants must also complete the following declarations.

- b) Will the project involve research related to [critical minerals](#) and/or one of the [critical infrastructure](#) sectors?
- c) Will the project involve the use of personal data or large datasets that could be considered sensitive (for additional information, see [List 2 of Annex A of the National Security Guidelines for Research Partnerships](#))?
- d) Will the project involve research related to goods or technology that are included on the [Export Control List](#) (ECL) of the Export and Import Permits Act (EIPA)?
- e) Will background intellectual property (IP) be transferred from Canadian institution(s) to the non-academic host organization(s)?
- f) Will intellectual property (IP) arising from the project be owned by, assigned to, or licensed to the non-academic host organization(s)?



If yes to any of declarations a) to f), Mitacs will assess potential research security risks and/or anticipated benefits to Canada. Mitacs will consider questions such as the following:

- Does the non-academic host organization have business operations, assets, and employees in Canada?
- Does the non-academic host organization have product or service offerings within Canada?
- Is the non-academic host organization owned or influenced by foreign governments?
- Is the non-academic host organization under [Canadian sanctions](#) or based in a country on the [Area Control List](#)?
- Has the non-academic host organization been identified by security agencies as a threat to Canada's national security?

Mitacs reserves the right to:

- Approve an application subject to additional conditions (e.g. submitting a satisfactory research security risk mitigation plan).
- Decline an application because of research security risks that cannot be mitigated.
- Decline an application because there are insufficient benefits to Canada.
- Request additional information to arrive at a decision on an application.

3. Mitigation of corporate research security risk

3.1 Dedicated resources

Mitacs has a dedicated Research Security Advisor within its Research Department to support the implementation of this Mitacs Research Security Plan. This resource supports the operationalization of the process outlined in section 2, 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.

3.2 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.

3.3 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 and 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.

4. Roles and responsibilities

The following table outlines the .

Roles	Responsibilities
Proposed and participating academic supervisor.	<p>Ensure the accuracy of own personal declaration regarding affiliations with/support from NROs.</p> <p>Ensure the accuracy of project declarations regarding STRAs, research security, and intellectual property (IP).</p>
Proposed and participating intern.	<p>Ensure the accuracy of own personal declaration regarding affiliations with/support from NROs.</p>
Proposed and participating non-academic host organization.	<p>Ensure the accuracy of information regarding the non-academic host organization that is submitted in Mitacs applications.</p> <p>Ensure the accuracy of project declarations regarding intellectual property (IP).</p>
Academic institution.	<p>Ensure that intellectual property (IP) arrangements conform to the policies of the academic institution.</p> <p>Ensure academic supervisors and interns are aware of any research security policies of the academic institution.</p>
Mitacs.	<p>Assess research security risks and benefits to Canada.</p> <p>Validate, as needed, the accuracy of project declarations regarding STRAs.</p> <p>Arrive at funding decisions on Mitacs applications.</p>