National Security Guidelines for Research Partnerships Risk Assessment Form

Save As | Print | Reset

Family name of applicant:	Initial(s) of all given names of applicant:	Grant administering institution:

This form must be used to assess potential risks that research partnerships may pose to Canada's national security as outlined in the Overview of the National Security Guidelines for Research Partnerships.

For additional information on risks, conducting a risk assessment, and mitigating risks, researchers may also consult the Safeguarding Your Research portal.

The risk assessment must be completed by researchers when submitting their applications for research partnerships involving private sector partner organizations to NSERC's Alliance Grants Program.

Private sector partner organizations are defined as for-profit organizations that support a research partnership by sharing in intellectual leadership or providing expertise or making cash and/or in-kind contributions underpinned by a formal agreement.

Partnership grant applications that are assessed by NSERC to be of higher risk will undergo a national security review, with engagement of national security departments and agencies, as well as members of the research community, as required.

Proposals assessed as posing a high national security risk will not be funded. Overviews of the process are found in Appendices A and B.

Risk Assessment Questionnaire

The following questionnaire will help you assess the potential national security risks associated with your proposed project. Answer the following sections to the best of your knowledge and using information and resources available to you. The circumstances of each partnership may require additional assessments or due diligence. Refer to the Safeguarding Your Research portal, relevant legislation, regulation, guidance, and other open sources that may help you answer these statements.

1. Know your Research

The research knowledge or intellectual property (IP) generated by this research could be of interest to foreign governments, militaries, or their proxies.	◯ Yes	◯ No	◯ Unsure
The field of research has potential military, policing, or intelligence applications, even if that is not your intended use for it.	◯ Yes	◯ No	◯ Unsure
The research falls under areas identified as sensitive (refer to Appendix A in the Overview of the National Security Guidelines for Research Partnerships).	◯ Yes	◯ No	◯ Unsure
You are working with areas covered by the Guide to Canada's Export Control List and the Nuclear Non-proliferation Import and Export Control Regulations.	◯ Yes	◯ No	◯ Unsure
You are working in research areas related to goods/technology identified in Section 35 of the *Defence Production Act* and known as the Controlled Goods List.	◯ Yes	◯ No	◯ Unsure
You are working in areas covered by the Export Control List, the Import Control List, the Area Control List, as amended from time to time (outlined in The Export and Brokering Controls Handbook). If yes, please see important note below.	◯ Yes	◯ No	◯ Unsure
You are working in research areas related to critical minerals and critical mineral supply chains (e.g., those included on the Government of Canada's Critical Minerals List).	◯ Yes	◯ No	◯ Unsure
You are working with sensitive personal data or large amounts of data that could be sensitive in the aggregate.	◯ Yes	◯ No	◯ Unsure
You are working in research areas focused on critical infrastructure (National Strategy for Critical Infrastructure and Action Plan for Critical Infrastructure).	◯ Yes	◯ No	◯ Unsure
The research facilities or infrastructure used to support the proposed project house sensitive data and/or provide access to infrastructure unrelated to this specific partnership	◯ Yes	◯ No	◯ Unsure

For any responses you answered **yes** or **unsure** to, please complete the Potential Risks Identified and the Risk Mitigation Plan sections below.

Important note (export controls):

Any transfer of physical items, software, or technology can constitute an export and is subject to the *Export and Import Permits Act* (EIPA). Depending on the item, software or technology, and the specific destination, an export permit may be required. Exports can include the return of loaned equipment, repairs of equipment, exchanges of samples and specimens, as well as transfers of instructions, test results, and preliminary findings. Intangible transfers of software and technology such as through e-mail or the cloud are also subject to requirements of the EIPA.

If this might apply to your research partnership, you should familiarize yourself with your obligations under the EIPA. The Export and Brokering Controls Handbook provides practical information about the administration of Canada's export controls pursuant to the Export Control List, the Brokering Control List, the Area Control List and the Automatic Firearms Country Control List, under the authority of the EIPA.

Recognizing that elements of research projects may change with time and that regulations can also change, it is your responsibility to stay abreast of changes to the EIPA and associated regulations. Should you believe these considerations are not applicable to your project, please check that box.

Know your EIPA obligations

I have reviewed the Export and Brokering Controls Handbook and I am aware of my obligations under the EIPA.	◯ Yes ◯ Not Applicable

2. Know your Partner *(consider <u>each</u> organization involved in the partnership)*

About your partner

Your partner organization, their parent organization, and/or their subsidiaries/affiliates have affiliations or partnerships that could lead to the transfer of research to third party governments, militaries, or organizations that could negatively impact Canada's national security.	◯ Yes ◯ No ◯ Unsure
Your partner organization, their parent organization, and/or their subsidiaries/affiliates could be subject to foreign government influence or control (e.g., there are policies and/or laws that compel knowledge transfer to that state).	◯ Yes ◯ No ◯ Unsure
There is an offer of funding where the ultimate source of the money and/or value to the funder is unclear.	◯ Yes ◯ No ◯ Unsure
There is an offer of funding which is conditional upon the researcher transferring to or replicating their work in a foreign country (e.g., setting up a mirror lab).	◯ Yes ◯ No ◯ Unsure
Your partner organization has been charged, admitted guilt, or has been convicted of fraud, bribery, espionage, corruption, or other criminal acts that could speak to a lack of transparency or ethical behaviour.	◯ Yes ◯ No ◯ Unsure
There is information to suggest that conflicts of interest or affiliations exist for any research team members that could lead to transfer of research to third party governments, militaries, or other organizations.	◯ Yes ◯ No ◯ Unsure
Your partner organization will have access to Canadian facilities, networks, or assets for conducting the research unrelated to this specific partnership.	◯ Yes ◯ No ◯ Unsure
Your partner organization is located in a country listed on the Area Control List (outlined in The Export and Brokering Controls Handbook).	◯ Yes ◯ No ◯ Unsure

For any questions you answered **yes** or **unsure** to, please also complete the Potential Risks Identified and the Risk Mitigation Plan sections below.

Potential Risks Identified

It is recommended that responses be no more than 500 words. Please provide the basis or information about any risks for which you provided a yes or unsure answer in the Risk Assessment Questionnaire. Describe the steps you have taken and resources you utilized to identify and assess the risks. (maximum 2,350 characters)

Risk Mitigation Plan

A risk mitigation plan must be developed, ideally, with support from your institution, to address risks identified via the questionnaire above or any factors that you are unsure about. The proposed risk mitigation plan will be assessed as part of the evaluation of the project proposal to ensure appropriate safeguards are in place to mitigate risks to the work.

It is recommended that responses be no more than 750 words. For all risks for which you answered yes or unsure in the Risk Assessment Questionnaire, describe what measures you will put in place to reduce the likelihood of the risk materializing and/or to lessen the impact in case the risk materializes. You must also provide a timetable for the implementation of the measures and discuss how you and your institution will monitor the effectiveness of these measures. (maximum 5,000 characters)

Categories of a risk mitigation plan are recommended to include:

- Building a Strong Research Team
- Assessing Alignment of Your Partners Motivations
- Ensuring Sound Cybersecurity and Data Management Practices
- Agreement on Intended Use of Research Findings
- Open Science approaches
- Other

Risk Mitigation

Mitigating Risks

Risk mitigation aims to reduce the likelihood and impact of risks to a level that is acceptable to the researcher, their institution, the granting agency, and the Government of Canada. Risk mitigation plans should describe actions that will be implemented to reduce risks' likelihood and impact.

Project Proposals Presenting Risks

A risk mitigation plan must be developed, ideally, with your institution, to address risks identified via the questionnaire above or any factors that you are unsure about. The proposed risk mitigation plan will be assessed as part of the evaluation of the project proposal to ensure appropriate safeguards are in place to mitigate risks to the work.

Examples of Risk Mitigation Measures include, but are not limited to:

- Training (research security, cyber security, and intellectual property training)
- Guidance and best practices from Government of Canada departments
- Partnership agreements that include intellectual property and technology transfer clauses that address national security risks
- Data management plan
- Cyber security plan
- Establishing access restrictions for partners and personnel to an "as needed" basis
- Regular reporting to your institution on the implementation and effectiveness of the proposed risk mitigation measures

The Government of Canada recognizes the importance of making Canadian science open to all, maximizing benefits for the well-being, health, and economy of our country. Open Science is the practice of making scientific inputs, outputs, and processes freely available to all with minimal restrictions. Scientific research outputs include:

(i) peer-reviewed science articles and publications,
(ii) scientific and research data, and
(iii) public contribution to and dialogue about science.

Open Science is enabled by people, technology, and infrastructure. It is practiced in full respect of privacy, security, ethical considerations, and appropriate intellectual property protection.

Additional guidance on principles, tools, and resources for research data management can be found in the Frequently Asked Questions of the Tri-Agency Data Management Policy.

You can also find guidance on best practices for risk mitigation on the Safeguarding Your Research portal in the guidance on Mitigating Economic and/or Geopolitical Risks in Sensitive Research Projects, which include:

Building a Strong Research Team:

Verify all team members' professional history and assess alignment with the research priorities for this project.
Conduct appropriate reference checks and due diligence on all members of the team. Are their credentials, publications and affiliations in line with what they told you? Consider asking colleagues who may have more direct knowledge of the individual than you, and review the individual's publication history and affiliations.

Assess existing or potential conflicts of interest or affiliation that would impede collaboration with any team members.
Ask yourself, "Could the interests or affiliations of my team members compromise the integrity of my research in a manner that jeopardizes Canada's national security?"

Discuss project risks internally and make a plan for their mitigation, involving external team members as appropriate.
Brainstorm potential project security risks with your team.

Assess whether the practices of your collaborator(s) and/or collaborating institution(s) are consistent with your institution's standards on ethics and research conduct.
Ask yourself whether all aspects of the project, regardless of where the work is or was performed, would pass ethics review at your institution.

Assessing the Alignment of Your Partners Motivations With Your Own:

Ensure the motivations of all partners are clear and aligned with the goals of the research team, including any expectations about intellectual property.
Ask the partner directly what they expect from the research team during the project and what they hope to get out of the project at the end.

Assess if the partner's governance structure is transparent and whether the ultimate beneficiary of their collaboration on your project is clear.
Looking on the partner's website, can you easily identify who leads the partner organization and any linkages to government, other organizations, and/or other actors? What information gaps exist?

Explore if other academics have had positive experiences collaborating with this partner.
By reaching out to researchers across your institution and at other institutions, you can gather valuable information on past experiences and solutions to address concerns.

Assess whether the practices and contributions of your partner(s) are consistent with the standards on ethics and research conduct at your own institution.
Ask yourself whether any contributions (data, background IP, etc.) are consistent with your institution's policies and/or Canadian laws.

Ensuring Sound Cybersecurity and Data Management Practices:

Verify that all team members have completed cyber hygiene and data management training.
Discuss appropriate training options with your CIO or with the relevant resource person in your institution.

Assess if the data management and cybersecurity measures needed to adequately protect research integrity are in place across all partners.
Consult your institution's policies and practices and internal research and IT services. Public Safety Canada and the Canadian Centre for Cyber Security offer resources and best practices.

Focus on addressing divergent cybersecurity and data management practices and decide on a mutually acceptable approach to securing your research data.
When reflecting on existing divergences, ask yourself, "Given the sensitivity of the research topic and data, what is the level of risk associated with a breach and what is the probability it may occur?"

If professional or personal international travel is expected during the project, agree to a protocol for device management.
See the Travel Security Guide for Researchers and Staff for more information.

Agreement on Intended Use of Research Findings:

Agree to a plan of how and when you will share details about the project, including publication, conferences, teaching, mass media, social media and personal communication. This will increase effectiveness and minimize disagreement later.
The UK's Health Foundation has a Communications in Health Care Improvement toolkit that could provide a good starting point. Keep in mind that premature disclosure can preclude certain types of IP protections.

Assess the potential value of any project- related IP and what you need to do to protect it.
Ask yourself, "What types of IP could be generated through this research project? What do we need to do to preserve the value of this IP?"

Ensure all collaborators and partners have agreed on how IP will be handled.
The appropriate contacts at your institution can help you understand your institution's policies with regard to IP, as well as how policies, laws and enforcement might vary across relevant institutions and countries.

Discuss how restrictions on academic freedom or commercial interests may impact the research project and the communication of research results.
Ask yourself, "Do the restrictions imposed on communicating results have potentially harmful impacts on the integrity of our research or our ability to publish results?"

Ensure all collaborators and partners are comfortable with the likely uses of any research results.
Brainstorm with your team the likely uses of the results of the project, then ask members if they remain comfortable proceeding with the project.

Ensure mechanisms exist that guarantee that any researcher involved in the project is able to use the results to complete their studies.
Verify with the appropriate contacts at your institution what measures exist at your institution and make all partners and collaborators aware of this requirement. Participants in NSERC-supported research must ensure that a researcher's graduation is not impeded by intellectual property issues, and must support the publication of results in the open literature. See the Policy on Intellectual Property for more information.

Open Science is the practice of making scientific inputs, outputs and processes freely available to all with minimal restrictions.
Adopt an open-by-design approach by incorporating a shared commitment by all research partners to identify and use best practices for Open Science at the start of the planning phase of research projects.

Appendix A: Overview of the Process

1. Researcher

a) The researcher fills the Risk Questionnaire and explains the rationale for identified risks. The researcher contributes to the development of the risk mitigation plan with the institution.

2. Research Institutions

a) The institution reviews and validates the Risk Questionnaire.
b) The institution supports the researcher to develop a risk mitigation plan to effectively address identified risks.
c) The Risk Questionnaire and the Risk Mitigation Plan, if applicable, are submitted with the grant application to the pertinent granting agency.

3. Granting Agency

a) The granting agency undertakes the scientific merit assessment of all research partnerships proposals it receives, as described in the funding opportunity's evaluation criteria and according to the established peer review process.
b) The granting agency reviews the Risk Questionnaire and the Risk Mitigation Plan (if applicable) provided with the grant application and, when necessary, refers the application for advice from national security partners.
c) For those applications that warrant examination of national security considerations, the granting agency will conduct an assessment of the risk level and refer specific applications to national security partners, should the initial risk assessment indicate a need to do so. Academic experts will be asked to provide input on the technical aspects of the subject matter and the effectiveness of proposed mitigation measures, as required.
d) The funding decision will take into consideration the scientific review as well as the assessment of potential national security considerations.

Appendix B: Process Flow Chart