

Title: Research security plan

Date of issue: December 2024

Category: Programs

Date of last revision: N/A

Approver: Board

Date of last review: N/A

Review frequency: Every three years

Research security plan

1. OVERVIEW

Genome Canada is strongly committed to the principle of rapid sharing of the outputs of Genome Canada-funded research including open access to publications, release of data and sharing of unique resources to the scientific community. As outlined in Genome Canada's [Data Release and Sharing Policies](#), providing the broader scientific community with timely access to the outputs of Genome Canada-funded projects will accelerate the translation of research for the benefit of Canada and the wider global community. However, research may be vulnerable to abuse through theft of data and cyber threats, as [communicated by Public Safety Canada](#). Breaches of sensitive or protected data can not only undermine the integrity of the research enterprise, but also impact Canadian national security, safety, and economic prosperity.

Genome Canada is committed to ensuring the security and integrity of its research initiatives. By adopting a comprehensive approach to research security, Genome Canada aims to protect sensitive information, intellectual property, and the overall integrity of its research projects. In line with the Government of Canada's [National Security Guidelines for Research Partnerships and the Policy on Sensitive Technology Research and Affiliations of Concern](#) Genome Canada has developed a research security plan and a process for all our funding programs to ensure that the Canadian research ecosystem is as open as possible and as secure as necessary. Through the implementation of this plan, Genome Canada not only safeguards its research but also contributes to the broader goal of maintaining Canada's leadership in genomics research and innovation.

2. PURPOSE

The purpose of Genome Canada's research security plan is to integrate national security considerations of the Government of Canada's [National Security Guidelines for Research Partnerships](#) and the [Policy on Sensitive Technology Research and Affiliations of Concern](#) into all of Genome Canada's funding programs.

3. SCOPE

The research security plan applies to all Genome-Canada funded researchers and their host organizations.

4. DEFINITIONS

Sensitive Technology Research and Affiliations of Concern (STRAC)

The Government of Canada's [Policy on Sensitive Technology Research and Affiliations of Concern](#) establishes guidelines to ensure that researchers applying for funding from Canadian federal agencies do not have affiliations with high-risk organizations, thereby safeguarding national security while advancing sensitive technology research areas.

National Security Guidelines for Research Partnerships (NSGRP)

The Government of Canada's [National Security Guidelines for Research Partnerships](#) aim to integrate national security considerations into the development, evaluation, and funding of research partnerships in Canada, ensuring that potential risks associated with collaborations—especially with private sector partners—are identified and mitigated to protect the integrity of the research ecosystem.

Private Sector Partner

A private sector partner is a for-profit organization, or an organization that assists, supports, connects and/or represents the common interests of a group of for-profit, incorporated organizations, such as an industry association or a formal or informal consortium.

5. PROCEDURES

The following apply to all applications received and projects funded by Genome Canada.

Sensitive Technology Research and Affiliations of Concern (STRAC)

Given that genomics and related technologies are on the list [sensitive technology research areas](#), it is assumed that all applications to Genome Canada's funding programs aim to advance a sensitive technology research areas. All researchers with named roles in the project are required to attest that they have read, understood, agree with, and are compliant with the Policy on Sensitive Technology Research and Affiliations of Concern and are not affiliated with, or in receipt of funding or in-kind support, from any of the institutions on the list of [Named Research Organizations](#) (see **Appendix I** for Genome Canada's research attestation form). The attestation form will be submitted through Proposal Central as part of all applications received by Genome Canada. Researchers with named roles on projects as well as their research team(s) will be required to comply with the policy for the duration of the funding.

As part of this policy, researchers should keep in mind that institutions that are not included on the Named Research Organizations list may still pose a risk to Canada's research and are encouraged to apply due diligence practices to mitigate risks that may be associated with any collaboration or partnership in a sensitive technology research area.

Genome Canada will validate, at a minimum, the attestations of all projects recommended for funding prior to the flow of funds.



National Security Guidelines for Research Partnerships

All projects recommended for funding must complete a [NSGRP Risk Assessment Form](#) and submit a risk mitigation plan if risks are identified via the risk assessment form or there are any factors that they are unsure about. The risk mitigation plan is intended to help the team members and the Institution(s) manage and respond to any risks arising within the project to address risks identified via the risk assessment form or any other factors that they are unsure about. The proposed risk mitigation plan will be signed off by the team and the host institution and be assessed by the Genome Centre before submission to Genome Canada to ensure appropriate safeguards are in place to mitigate risks to the work.

For funded projects that are affiliated with, or in receipt of funding or in-kind support from a private sector partner, a Private Sector Partner Identification Form (**Appendix II**) must also be submitted per private sector partner.

Genome Canada will validate the information provided by researchers and research partners on the NSGRP Risk Assessment Form and Private Sector Partner Identification Form(s) (if applicable) for all projects recommended for funding prior to the flow of funds using guidance provided by ISED in Conducting Open Source [Due Diligence for Safeguarding Research Partnerships](#). Genome Canada will seek guidance from ISED on any research and/or research partners that are deemed to pose a national security risk.

Management of funded projects

Genome Canada-funded researchers are expected to comply with the STRAC Policy and the NSGRP for the duration of their projects. Researchers should continue to follow the best research practices in accordance with Genome Canada's [Guidelines for Funding](#) and [Data Release and Sharing Policies](#) as well as the [Tri-Agency Framework: Responsible Conduct of Research](#). Through these policies, and in coordination with federal departments and agencies as well as other third-party national research organizations, Genome Canada is committed to maintaining the highest levels of research excellence and integrity, academic freedom and openness, and the proper stewardship of public funds.

If needed, information on safeguarding research, on conducting risk assessment and on best practices for traveling internationally is available on the Government of Canada's [Safeguarding your Research](#) portal.

Research security and risk mitigation strategies will be monitored throughout the lifetime of the project as part of progress reporting and Genome Canada's change management guidelines. If any changes occur that may impact research security risk during project terms (e.g., new project team member, changes to private-sector partners) researchers must submit applicable forms for validation through the regional Genome Centre to Genome Canada.

Updates and changes to the status of a project, including the addition of new partners or changes in the geopolitical landscape, may trigger the need for an updated mitigation strategy.



Genome Canada reserves the right to withdraw funding to any project should risk(s) to research security be identified.

6. ROLES AND RESPONSIBILITIES

Researchers

- All researchers involved in activities supported by Genome Canada funding must ensure they remain compliant with the Policy on STRAC and the NSGRP for the duration of funding.
- All researchers must inform Genome Canada, through their Genome Centre, of any changes that may impact compliance with the Policy on STRAC and the NSGRP.

Academic institution

- Academic institutions must conduct risk assessments and ensure compliance with STRAC and NSGRP guidelines for sensitive technology research at the application stage and for the duration of a project term. They are responsible for providing training on these policies, implementing security measures, and maintaining transparency in research activities.

Genome Centre

- The Genome Centres will work with researchers and Institutions in completing the risk assessment form and risk mitigation plan, ideally, with support from the host institution(s).
- Assess risk mitigation plans submitted by researchers to ensure appropriate safeguards are in place to mitigate risks prior to submission to Genome Canada.

Genome Canada

- Genome Canada will assess potential research security risks and seek guidance from ISED on any research partners that are deemed to pose a national security risk.
- Genome Canada will validate the accuracy of attestation forms and risk assessments received and seek guidance from ISED on any research partners that are deemed to pose a national security risk.
- Complete ongoing research security training sessions for Genome Canada staff to ensure research security risk is understood and compliance with the Policy on STRAC and the NSGRP is maintained.
- Continue communications and engagement with research security advisors within other Strategic Science Fund organizations, the Tri-Council, ISED and other research security working groups to ensure Genome Canada is prepared to respond to new threats and any changes to the Government of Canada's research security policies.

DOCUMENT HISTORY

Action

Research Security Plan issued

Date

December 12, 2024



Attestation for research aiming to advance sensitive research technology areas

Researcher information

Last name: _____ First name: _____

Primary affiliation: _____

Email address: _____

Public profile link (optional) – for the purpose of identification. Any public profile can be provided, including but not limited to ORCID, Google Scholar, ResearchGate, LinkedIn, or a personal or institutional webpage.

Attestation

As of the date of this attestation, I attest by completing this form that I have read, understood, and am compliant with the [Policy on Sensitive Technology Research and Affiliations of Concern \(STRAC\)](#).

Funding applications submitted to Genome Canada will not be funded if any of the researchers involved in activities supported by the funding are currently affiliated with or in receipt of funding or in-kind support from any of the listed [Named Research Organizations \(NRO\)](#).

I understand that:

- This attestation form is required because Genome Canada funding advances a listed [Sensitive Technology Research Area \(STRA\)](#).
- By completing this form, I take responsibility for the accuracy of my attestation statement.
- All information provided in this form will be stored securely and may be shared with Government of Canada departments and agencies at any time for the purpose of national security assessment to validate compliance with the policy.
- Should the funding be awarded, compliance with the [STRAC policy](#) as defined at the time of application will be required for the duration of the funding.
- Actions may be required if there are changes to the nature of the research or to the composition of the research team.
- Non-compliance with this policy may represent a breach of the [Tri-Agency Framework: Responsible Conduct of Research](#)

Signature

As of the date of attestation on this form and to the best of my knowledge, I attest that by my signature, I am not affiliated with or in receipt of funding or in-kind support from any of the listed [Named Research Organizations \(NRO\)](#). I also understand that all researchers involved in the activities supported by this grant must comply with the [Policy on Sensitive Technology Research and Affiliations of Concern \(STRAC\)](#), as defined at the time of application, for the duration of this funding.

Date:

Signature:



Private-sector partner identification form

Organization:	
Operating as (if different than organization's legal name):	Business number:
Organization's website:	
Has business operations in:	Worldwide headquarters located in:
If applicable, indicate the parent company's name:	
Indicate if the organization is incorporated in Canada (either federally or provincially/territorially):	Date of incorporation (if applicable):
Indicate up to three sectors the organization is involved in: 1. 2. 3.	
Department or branch involved in the project:	
Contact information	
Last name:	First name:
Position:	
Email address:	
Phone number:	



Partner organization's contribution to the research project	Yes	No
The private-sector partner has an active role in the research activities described in the funding proposal (e.g., sharing of intellectual property, providing expertise, actively participating in research activities, contributing financially to the research activities).		
The private-sector partner will be providing co-funding		
The private-sector partner will plan to retain Intellectual Property related to research in the funding proposal		

Employees involved in the project, if applicable	
Last name:	First names:
Position:	
Email address:	
Last name:	First names:
Position:	
Email address:	
Last name:	First names:
Position:	
Email address:	
Last name:	First names:
Position:	
Email address:	
Last name:	First names:
Position:	
Email address:	

