



**Stem Cell
Network**

Powering
Regenerative
Medicine

**Réseau de
Cellules Souches**

Propulsons
la médecine
régénératrice

Guidance on Research Security for SCN Funding Applications

July 2026

All applications submitted to the Stem Cell Network (SCN) must comply with the Government of Canada's [Policy on Sensitive Technology Research and Affiliations of Concern \(STRAC\)](#) and the [National Security Guidelines for Research Partnerships](#) (NSGRP).

In alignment with the Government of Canada's STRAC Policy, applications involving research that aims to advance a [Sensitive Technology Research Area](#) (STRA) must comply with the policy's eligibility requirements. Regenerative medicine (including tissue engineering and gene therapy) is identified as a Sensitive Technology Research Area. Accordingly, all researchers (Lead Investigator, co-investigators, collaborators, and Highly Qualified Personnel) must be informed of the STRAC Policy, the [Named Research Organizations](#) (NRO) list, and SCN's Guidance on Research Security. SCN also **requires submission** of the Tri-Agency STRAC Attestation Form for all named researchers (Lead Investigator, co-investigators, and collaborators). SCN reviews recommended applications for compliance with the STRAC Policy.

NSGRP applies to research involving Sensitive Technology Research Areas where the project includes an eligible private-sector partner (i.e., organizations that are not owned or operated by any order of government and includes all for-profit organizations). Applications proposing projects involving eligible private-sector partners should ensure they are familiar with the NSGRP requirements and **must submit** a completed Government of Canada's NSGRP Risk Assessment Form. SCN reviews these applications in accordance with NSGRP to assess research security risks and determine whether additional information or mitigation measures are required.

Where discrepancies, omissions, or potential research security concerns are identified, applicants may be asked to provide clarifications, updated documentation, or revised information before final funding decisions are made.

1. SCN'S RESEARCH SECURITY PROCESS FOR APPLICANTS: RESEARCHER RESPONSIBILITIES:

- a. All researchers (lead-investigators, co-investigators, collaborators and HQP) involved in activities to be supported by an SCN funding application must be informed of [Named Research Organizations](#) and be aware of their individual responsibilities with regards to compliance with the STRAC Policy.
- b. At the application stage, all named researchers (lead-investigators, co-investigators, and collaborators) must each complete the [Tri-Agency STRAC attestation form](#) stating that they are not currently affiliated with or in receipt of funding or in-kind support from any of the listed institutions on the NRO. The lead-investigator is responsible for gathering these forms from all researchers into a single PDF and submitting with the funding application.
- c. For applications involving one or more private sector partners, the lead investigator must complete and upload a [Government of Canada's NSGRP Risk Assessment Form](#) with the application that covers each private-sector partner included in the project. Lead investigators should consult Government of Canada resources, which provide practical [guidance](#) and [training](#) (including the "[Safeguarding Research Partnerships with Open Source Due Diligence](#)" course) to conduct open source due diligence testing for partners and help complete the risk assessment form. Only one risk assessment form is required to be uploaded per application.
- d. Applicants are advised that all funded lead investigators and co-investigators must complete the Government of Canada's foundational research security training courses, including [Introduction to Research Security](#), [Dual-Use in Life Science Research](#), and [Insider and Outsider Threats](#). Completion certificates are not required at the application stage but are required as a condition of funding prior to the release of SCN funds.

2. POST AWARD REQUIREMENTS:

If an application is funded by SCN, the following conditions and responsibilities will apply for the duration of the award:

- a. Award recipients and research team members must maintain compliance with the Government of Canada's STRAC Policy and, where applicable, the National Security Guidelines for Research Partnerships (NSGRP).
- b. Award recipients must notify SCN of any material changes to the project team, named researchers, collaborations, private-sector partners, or other circumstances that may affect research security compliance. Researchers will also be asked to confirm these changes through SCN's annual Continual Review process.

- c. Award recipients are responsible for ensuring that all research team members are informed of their responsibilities under the STRAC policy and, where applicable, NSGRP, as well as the Named Research Organizations (NRO) list and SCN's Guidance on Research Security. This responsibility extends to any individuals who join the project after the award is made. Where required, newly added named researchers must submit a completed Tri-Agency STRAC Attestation Form.
- d. Where changes to a project involving a private-sector partner affect the information provided in the original Government of Canada's NSGRP Risk Assessment Form, the Lead Applicant must notify SCN and submit an updated NSGRP Risk Assessment Form and supporting documentation, where required.
- e. As part of SCN's annual Continual Review process, award recipients will be asked to confirm ongoing compliance with SCN's research security requirements, including changes to the project team or private-sector partners, the addition of new HQP, and the submission of any required updated research security documentation.

Research security compliance is monitored throughout the application and award period. Where concerns are identified, SCN may request additional information or updated documentation to support its assessment. Depending on the nature and severity of the concern, unresolved or ongoing non-compliance may result in corrective actions, funding modifications, suspension or termination of funding, or other measures in accordance with SCN's Research Security Policy.