OFFICE OF RESEARCH AND INNOVATION

NIPISSING UNIVERSITY

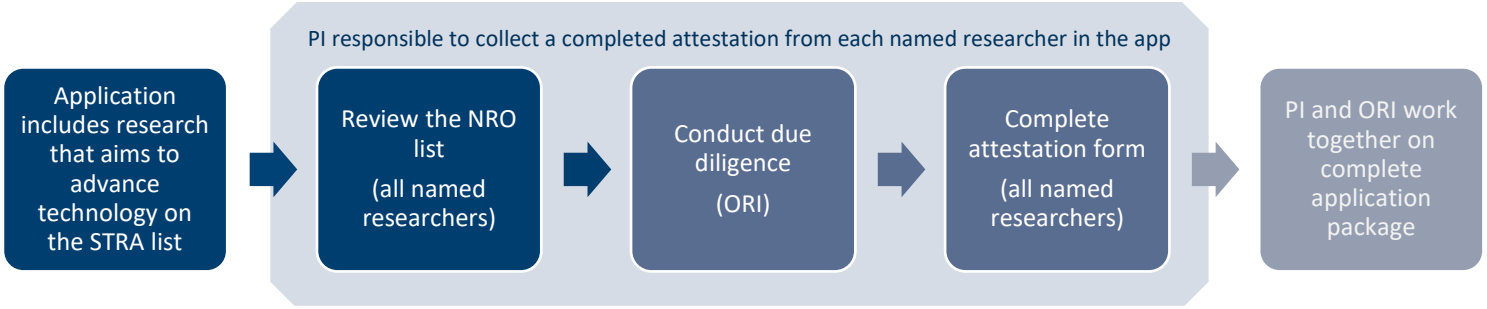
Research Security Quick Guide

Research security involves identifying potential risks to your work, such as unwanted access, interference, or theft, and implementing measures to mitigate these risks. It is essential to safeguard the inputs, processes, and outcomes of scientific research and discovery. Research security is a collective responsibility that applies to all individuals involved in the research ecosystem. By prioritizing research security, we ensure the integrity and protection of our scholarly activities while meeting institutional, funding agency, and research partner requirements, and federal and provincial policies. This quick guide provides information about existing research security requirements that apply to Tri-Agency and Ontario research funding programs. The Office of Research and Innovation (ORI) is available to support researchers with inquiries concerning any research security requirements that apply to other funders and when completing government sponsored research contracts.

FEDERAL APPLICATIONS

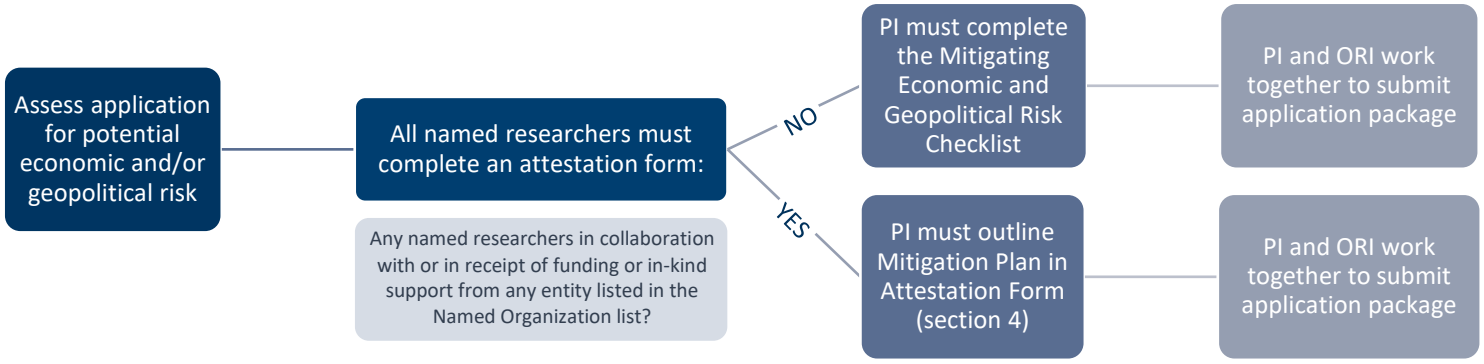
The STRAC policy applies to all Tri-Agency and CFI funding opportunities.

ORI: Office of Research & Innovation
STRA: Sensitive Technology Research Areas
NRO: Named Research Organization



All researchers are encouraged to use the National Security Guidelines for Research Partnerships (NSGRP) to assess all research partnerships, with any partner or funder, to protect their work. The NSGRP will be applied to CFI and other relevant federal research partnership funding opportunities. These guidelines provide clear information on the specific national security considerations for research partnerships. Accompanying resources guide researchers through conducting a risk assessment and working with research partners and universities in creating a risk mitigation plan.

PROVINCIAL APPLICATIONS



Provincial vs. Federal research security processes

- The Ontario government requires attestation from all Named Researchers in all applications to all Ministry programs, whether the research is classified as sensitive or not, and whether researchers are associated with Named Research Organizations or not.
- The Ontario government allows applicants with high-risk proposals to propose a risk mitigation plan, which, if approved, may render that project fundable.

Application Attestation Form

Mitigating Economic and Geopolitical Risk Checklist

RESPONSIBILITY OF INSTITUTION

PRE-AWARD

Research Security Support

The Office of Research and Innovation (ORI) provides both pre and post award support, including ensuring adherence to research security requirements. ORI provides guidance and assistance with:

- ✓ Attestations and related documentation
- ✓ Risk assessment and due diligence
- ✓ Mitigation plans
- ✓ Sharing relevant resources and best practices

Internal Application Review

To align with institutional and Tri-Agency requirements, applications requiring attestations will not be approved for submission unless all attestations are complete.

Researchers must adhere to ORI's pre-submission timeline:

1 **1st Submission** Application draft, including attestations
Due 3 weeks prior to external deadline

2 **Resubmission** Final application with all required edits
Due 2 business days prior to external deadline

POST-AWARD

Federal

ORI will support the PI to ensure understanding of the terms and conditions of awarded grants. This includes helping the PI navigate the following situations:

- The nature of the research evolves such that activities supported by the grant would aim to advance a listed Sensitive Technology Research Area; and/or
- The composition of the research team changes, requiring the submission of attestation forms from newly added members.

Provincial

Approved projects are conditional upon the Applicant entering into a Ministry Transfer Payment Agreement (TPA), which now includes specific terms and conditions regarding research security matters. The TPA will include additional terms for projects deemed high-risk, outlining specific risk mitigation requirements. ORI will help the PI navigate changes in information provided in the Risk Mitigation Form for the PI or other named researchers connected to the project.

RESOURCES

POLICIES

Policy on Sensitive Technology Research and Affiliations of Concern (STRAC)
List of Named Research Organizations (NRO)
Sensitive Technology Research Areas (STRA)
National Security Guidelines for Research Partnerships (NSGRP)
Tri-agency Guidance on the Policy on Sensitive Technology Research and Affiliations of Concern
Tri-agency guidance on the National Security Guidelines for Research Partnerships
Tri-Agency Framework: Responsible Conduct of Research

ATTESTATIONS, ASSESSMENTS

Application Attestation Form for Researchers Applying to Ontario Research Funding Programs
Mitigating Economic and Geopolitical Risk Checklist (Ontario)
Tri-Agency's Attestation for Research Aiming to Advance Sensitive Technology Research Areas
CFI's Attestation for Research Advancing Sensitive Technology Research Areas
The National Security Guidelines for Research Partnerships' Risk Assessment Form

QUESTIONS?

For further guidance or any research security inquiries, please visit Nipissing University's webpage, Safeguarding Your Research or contact research@nipissingu.ca.