ArcticNet
ᐅᑭᐅᖅᑕᖅᑐᒥᒃ ᑐᑭᓯᓂᐊᖅᑲᑎᒌᑦ

External Research Security Policy for Ultimate Recipients

1. Purpose

The ArcticNet External Research Security Policy (the “**Policy**”) governs and supports the ArcticNet’s research security activities related to its funding programs for Ultimate Recipients (URs).

2. Objective

The objective of this Policy is to define for URs their responsibilities with regards to Research Security.

3. Approval and authority

The ArcticNet’s Board approves this Policy and any revisions or amendments to it. The Policy is reviewed on a bi-annual basis.

Ultimate authority for operationalization of this Policy resides with the ArcticNet’s Chief Executive Officer (CEO)/ Executive Director (ED).

4. Definitions

Eligible Project: means a project undertaken by a UR in support of ArcticNet’s objectives within the parameters of the UR Funding Agreement.

Research Security: refers to the actions that safeguard the integrity of research domestically and internationally, with a particular emphasis on protecting against threats to national and economic security.

Research Security Incident: refers to any event that compromises the confidentiality, integrity or availability of research data, including unauthorized access, data breach or loss of research materials.

Sensitive Research*:* includes dual-use research, meaning products, data, knowledge, or technologies that, although developed and/or collected for legitimate purposes, have the potential to be illicitly acquired and/or exploited by others to purposely cause harm or to threaten public health or national security. It also includes new and emerging technologies for which their potential military/security and intelligence applications are less clear or well-known, research areas related to critical minerals and critical mineral supply chains, research areas that involve personal data, and research areas focused on critical infrastructure.

Service Provider: means a third party with whom a UR, or one of the participants involved in a project, has entered into agreements for services, facilities and/or infrastructure that are necessary to support project activities.

Ultimate Recipient (UR): means an organization of one of the following types selected by ArcticNet to receive funding to carry out an Eligible Project:

- post-secondary institutions;
- the private sector;
- Canadian post-secondary institutions;
- Indigenous organizations and governments;
- research networks;
- research hospitals;
- municipalities;
- public engagement networks; and
- not-for-profit organizations.

Ultimate Recipient Funding Agreement (URF Agreement): means an agreement entered into between ArcticNet and a UR for funding to be provided by ArcticNet for an Eligible Project.

5. Statement of commitment

ArcticNet is committed to fostering a secure research environment. It requires URs to commit to exercise research security due diligence by implementing necessary security measures to protect research activities and data.

Unauthorized access to sensitive research can undermine Canada's national security interests or those of its allied countries by negatively impacting Canada's capacity to identify and respond to these threats, or by disrupting the Canadian economy, society, and critical infrastructure. For a list of sensitive research areas that Canada's national security agencies have identified as having specific potential for dual-use or for being targeted by foreign governments, militaries, their proxies, or other actors for the potential to advance national security capabilities and interests see *Annex A of the National Security Guidelines for Research Partnerships.*

ArcticNet requires URs to commit to ensuring that research security planning is undertaken.

In addition, URs must abide by applicable laws and other binding authorities such as standards, accreditations, and professional orders, as well as ArcticNet policies and procedures. In addition, they must respect the Tri-Agency Research Data Management Policy, the federal Guidance for Research Organizations and Funders on Developing a Research Security Plan, and the National Security Guidelines for Research Partnerships.

6. Research security requirements

The following section outlines ArcticNet's expectations and requirements of URs in relation to research security.

7. Cybersecurity

ArcticNet requires URs to ensure that their research security measures are aligned with their institutional/organizational cybersecurity policies and processes, as well as any cybersecurity requirements that may be specified by ArcticNet.

8. Data management

ArcticNet requires URs to develop and maintain data management plans. For more information on this requirement, see ArctictNet's Data Management Policy.

URs who work with data created in the context of research by and with Inuit, First Nations, and Métis communities, collectives and organizations, must ensure the data are managed according to principles developed and approved by those communities, collectives and organizations, and in partnership with them.

9. Evaluation

ArcticNet is committed to reviewing UR research security measures to ensure they meet the requirements outlined in this Policy. Upon application for funds, the URs who intend to advance research that constitutes a Sensitive Technology Research Area, they must fill in the Sensitive Technology Research Areas form provided by ArcticNet for each team member. Additionally, if the project includes partners, private or other, that meet the definition below (based on the Canadian Foundation for Innovation (CFI) definition below), they have to provide a Risk Assessment Form and a partner identification form.

o Private-partner or partner definition:
Has an active role in the research activities described in the proposal (e.g., sharing of intellectual property, providing expertise, actively participating in research activities, contributing financially to the research activities); or Houses part or all of the research infrastructure; or Contributes more than $500,000 to the infrastructure through a cash or in-kind contribution to any single item.

ArcticNet will review all applications associated with the Calls for Proposals and identify any missing STRA forms, Risk Assessment Forms, or other required documents. If projects are deemed at medium or high risk, ArcticNet will ask the URs to identify risk mitigation measures to reduce risk. ArcticNet will engage with the UR's research support organization if any concerns remain. Reviews of the URs' research security measures for research that constitutes a Sensitive Technology Research Area will be required with annual progress reports submitted to ArcticNet by URs.

Intellectual property
All IP derived from data, including anonymized data, datasets, labelled data, representations, trained models and outputs, are considered eligible project IP and subject to the commitments and requirements of ArcticNet's Intellectual Property Policy.

10. Location and protection

URs confirm that any sensitive data of theirs or of any participants involved in their project are hosted on servers located in Canada. They also confirm that they are maintaining appropriate technical and organizational security measures to protect data from unauthorized loss, use, disclosure, alteration, or access and complying with any security measures that may be specified by their institution/organization and ArcticNet.

If URs and any participants involved in their project retain the services of a service provider for the hosting of their sensitive data, the sensitive data is still hosted on servers and facilities in Canada that are owned, controlled and operated by the service provider. URs and any participants involved in their project use reasonable efforts to ensure that the service provider is subject to information security controls at least substantially similar to those required under the UR agreement.

11. Monitoring

URs are responsible for ensuring that research security risks, assessments, and mitigation measures are tracked and monitored on an ongoing basis and in a manner that is consistent with their institutional/organizational research security policies and processes, and with the requirements of this policy.

12. Reporting

URs must report promptly to ArcticNet any changes in research scope or partner affiliations that could affect research security risk levels, as well as their planned mitigation measures.

13. Research security incident

URs and the participants involved in their project notify ArcticNet without undue delay and no later than twenty-four (24) hours upon becoming aware of a research security incident in relation to an ArcticNet funded project. This notice shall minimally include a description of the:

- nature of the research security incident, including the incident type;
- likely consequences of the research security incident; and
- measures taken or proposed to be taken by URs and the participants involved in their project to address the research security incident, including, where appropriate, measures to mitigate possible adverse effects.

Once ArcticNet has received notification of a research security incident, it notifies its funders.

If complete information is not available at the time of the initial notification, URs must provide updates to ArcticNet as the information becomes available, ensuring full disclosure of the incident. Furthermore, URs must document all responsive actions taken and conduct a post-incident review to assess and analyze the events and measures implemented. Once completed, this documentation is shared with ArcticNet.

14. Research security management

The following ArcticNet's expectations and requirements of URs in terms of their research security management:

Know your research

URs are required to review the Government of Canada's list of sensitive technology research areas (STRA) to determine if their research aims to advance any of the areas. If their research falls within a STRA, URs must complete an attestation form and share it with ArcticNet. This form requires them to certify that they are not affiliated with, nor have been funded o supported by, any of the Government of Canada's Named Research Organizations (NROs).

Know your partner involved in your projects

URs are required to assess the risks associated with private-sector partners involved in their projects. This assessment should determine if the research project involved a private-sector partner that plays an active role in the project and/or supports the research partnership through financial (cash) or non-financial (in-kind) contributions. If a private-sector partner is involved, URs must disclose the partner's affiliations and develop a comprehensive risk mitigation plan to address any potential Research Security concerns. This should be documented using the risk assessment form and submitted to ArcticNet.

Know the Research Affiliations of your research team
URs must disclose the research affiliations of all members of their research teams to ArcticNet. ArcticNet will then verify that these affiliations do not include any Named Research Organizations (NROs).

15. Non-compliance

Failure to comply with this Policy may result in sanctions, including but not limited to, suspension or termination of funding. ArcticNet reserves the right to take necessary actions to enforce compliance.

16. Contact information

Amendment: The Board may amend this policy.	Last Review:
Approval Date: Not approved as it is an operational policy, but the Board agreed with this version. March 11, 2025.	Last Revision: