Innovation, Science and Economic Development Canada
Innovation, Sciences et Développement économique Canada
Canada

Guidance for Research Organizations and Funders on Developing a Research Security Plan

This publication is available online at https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/guidance-research-organizations-and-funders-developing-research-security-plan.

To obtain a copy of this publication, or to receive it in an alternate format (Braille, large print, etc.), please fill out the Publication Request Form at www.ic.gc.ca/publication-request or contact:

ISED Citizen Services Centre

Innovation, Science and Economic Development Canada

C.D. Howe Building

235 Queen Street

Ottawa, ON K1A 0H5

Canada

Telephone (toll-free in Canada): 1-800-328-6189

Telephone (international): 613-954-5031

TTY (for hearing impaired): 1-866-694-8389

Business hours: 8:30 a.m. to 5:00 p.m. (Eastern Time)

Email: ISED@canada.ca

Reproduction Authorization

Cat. No. Iu37-38/2023E-PDF

ISBN 978-0-660-47274-4

Aussi offert en français sous le titre *Lignes directrices à l'intention des organismes de recherche et de financement sur l'élaboration d'un plan de sécurité de la recherche*.

Table of Contents

Preface

Research organizations and funders[1] play a significant role in diversifying and strengthening Canada's research ecosystem by conducting and funding research projects and partnerships that contribute to our country's social and economic well-being. The Government of Canada is committed to ensuring that these organizations have the support and tools necessary to safeguard their work, and/or the work that they support, from foreign interference, espionage, theft, and unwanted knowledge transfer. It is important for research organizations and funders to safeguard their research to ensure that it is not exploited in unintended or undesirable ways. The negative impacts of inadequate research security can include diminished trust and confidence in research data and results; loss of research data; loss of control over intellectual property, patent opportunities, and potential revenue; legal or administrative consequences; loss of potential future partnerships; and/or tarnished reputation. Research security policies and practices in Canada aim to prevent Canadian innovation from being used to advance the military weapon systems and surveillance technology of hostile states. In recognizing that threats towards Canadian research are evolving and come in many forms, a collective effort is required to develop Canada's research security resiliency – researchers, research organizations, funding organizations, and governments all share the responsibility of identifying and mitigating national security risks related to research partnerships.

This guidance document supports the Government of Canada's commitment to research security, which includes maintaining the foundational principles of open science and academic freedom. Open science and research security are complementary and mutually reinforcing, and this balance is necessary to ensure that research benefits Canada and all Canadians. Complementary guidance can be found on the Safeguarding Your Research portal, including the *National Security Guidelines for Research Partnerships*.

Please note that this guidance document is intended for research organizations and funders who are not currently required by the Government of Canada to implement the Risk Assessment Form under the *National Security Guidelines for Research Partnerships.*

[1] Funders are defined as organizations that distribute money to recipients (organizations or individuals) that conduct or support research projects and related activities such as research training.

1. Purpose

The purpose of this document is to provide research organizations and funders with guidance on how to exercise research security due diligence by developing and implementing a research security plan that establishes a process for the identification, assessment and mitigation of national security risks in a systemic, consistent, and documented manner. More specifically, this guide will assist research organizations and funders in demonstrating how they can:

- Identify and analyse risks associated with the types of research projects they conduct and fund that involve partnerships, and determine the threats affiliated with any implicated research partners; and
- Develop and implement a series of tailored research security best practices and mitigation measures at the project and organization level that are both feasible and risk proportionate.

While the focus of this document is on research organizations and funders, the principles and practices outlined within this guide should be applied and adapted – when necessary – to inform the development of security plans for organizations that support or engage in other related activities including training, technology transfer, or business development.

2. Components of a Research Security Plan

2.1 Research Security Plan Objectives

A research organization or funders' *Research Security Plan* should support and complement the Government of Canada's overarching country and company agnostic approach to research security. The sections below describe the key components of a comprehensive *Research Security Plan*, which supports the integration of national security considerations into research and funding practices. This includes:

- Assessing the sensitivity of the research, including whether research could be at risk or targeted for theft, espionage or foreign interference;
- Assessing the risk level of any partners organizations involved in the research;
- Assessing the research or funding organization's existing security posture; and
- Developing and implementing effective risk mitigation measures to address risks identified.

2.2 Know the Research You Fund or Conduct

Research organizations and funders should to have a clear understanding of the research and projects they conduct or fund, as well as their potential respective applications (military and civilian), to appropriately assess the level of national security risk and determine which assets should be protected.

In the context of this document, sensitive research – as well as its underlying data and resulting technologies – are defined as research and technologies which could be used to advance a foreign state's military, intelligence, or surveillance capabilities. 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. Sensitive research includes dual-use research, which refers to 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. Sensitive research also includes new and emerging technologies where their potential military/ security and intelligence applications are less clear and well-known, as well as research areas related to critical minerals and critical mineral supply chains; research areas that involve personal data; or research areas focused on critical infrastructure.

See **Annex A** of the *National Security Guidelines for Research Partnerships* for a list of the 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.

For more information on risks associated with sensitive research, please consult the "*Assessing Your Risk Profile*" webpage located on the Government of Canada's *Safeguarding Your Research Portal*.

2.3 Know Your Partners

Research funders and organizations should to be aware of and assess risks associated with partner organizations that may be involved in the research they fund or conduct. This includes the risk that the partner may transfer the research knowledge, data, or results to a foreign government, military, their proxies, or other actors where doing so may harm Canada's national security interests.

Partner organizations that are state-owned or subject to state-influence could facilitate unauthorized knowledge, technology, or intellectual property transfer to foreign governments, militaries, their proxies, or other actors, in a manner that could harm Canada's national security. This risk is especially high for partner organizations associated with countries that have laws or practices that compel entities and individuals to be subject to direction from their governments. Such partner organizations lack autonomy and independence and can be directed by foreign governments to relinquish any Canadian or international information, research knowledge, technology, and associated intellectual property.

Risks can also originate from partner organization personnel participating in a project, particularly if individuals have ties to foreign militaries, governments, or institutions that are known to engage in unauthorized knowledge transfer. Their influence over and access to data and infrastructure (both physical and digital) could be used to support unwanted data access or knowledge transfer outside the scope of the research partnership.

See **Annex B** of the *National Security Guidelines for Research Partnerships* for additional factors that may result in an elevated risk of unwanted knowledge transfer to a foreign government, military, their proxies, or other actors.

For more information on identifying risks associated with research partnerships, please consult the "*What are the national security risks in research partnerships*" webpage located on the Government of Canada's *Safeguarding Your Research Portal.*

2.4 Know Your Organization's Security Posture

To protect core assets, including research data and results, research organizations and funders are encouraged to proactively assess their existing security posture at the organizational level. An organization's security posture refers to its overall readiness and ability to prevent, detect and respond to threats or attacks. It is good practice to identify other areas of vulnerability within an organization's infrastructure and business processes that could contribute to unauthorized access to research methods, techniques, and results. To effectively safeguard research and intellectual property that is owned or financed by a research organization or funder, it is beneficial to identify and evaluate organizational areas of risk, including:

- **Physical Security:** Instituting appropriate physical security controls can reduce the risk of unauthorized access to identified assets and other sensitive materials.
- **Personnel Suitability and Reliability**: Assessing an individual's current and ongoing suitability for a position can reduce the risk that an individual with access will compromise assets**.**
- **Information Management and Cyber Security:** Protecting sensitive information from unauthorized access or theft and ensuring the requisite level of confidentiality can reduce the risk of unintended information transfer.
- **Incident and Emergency Response:** Reporting and responding appropriately to events that have the potential to cause harm to information, personnel, the research community, or the physical working environment can help to mitigate and reduce the magnitude of incidents when they occur, as well as reduce the risk of recurrence.

Understanding the Sources of Threats

Threats can come from individuals or groups both within and outside an organization. **Insider threats** can include anyone who has knowledge of, or access to, an organization's infrastructure and information and who could inadvertently or knowingly exploit this access for illegitimate purposes or to cause harm. **Outsider threats** encompass individuals or groups that do not have authorized access to an organization's assets, but who act in a way that could lead to the illegitimate acquisition of assets and to subsequent harm.

For example, research facilities that undertake and store their work on site can be targeted by threat actors seeking to gain access to their research data, information, knowledge, and/or infrastructure. Threat actors can use a variety of methods that include, but are not limited to, taking pictures of the facility or documents housed within, theft of digital information through portable storage devices (e.g. USB), or gaining access to restricted areas by taking advantage of ineffective physical security barriers.

Digital research data can also be targeted by threat actors through ransomware, phishing, and other cyber-attacks that take advantage of vulnerabilities in infrastructure or cyber security practices to access research data, information, or knowledge that would not otherwise be publicly available.

2.5 Identify Risk Mitigation Measures

Research funders and research organizations should identify and apply measures that can help minimize identified security risks to safeguard their funded research and its intended outcomes. This includes establishing organizational-level risk mitigations, and where necessary, project-level risk mitigations. In cases where the risks to Canadian interests cannot be sufficiently mitigated or where the risks outweigh the potential benefits, those research projects or partnerships should not be funded or proceed.

All organizations, projects, and programs are unique. Some may already be sufficiently mitigated by policies and measures already in place, while others may require different levels of additional risk mitigation. Ultimately, risk mitigation should be proportional to the level of risk. Research organizations should familiarize themselves with the many types of practical mitigation measures that can be adopted to address risks.

For more information on potential mitigation measures that can be applied to research projects, please consult the guide titled "*Mitigating economic and/or geopolitical risks in sensitive research projects*" located on the Government of Canada's *Safeguarding Your Research Portal.*

3. Research Security Governance Framework

Each research organization and funder is unique and conducts or funds an array of research programs that present varying levels of risk to research security.

As part of developing a *Research Security Plan,* research organizations and funders should conduct an internal scoping exercise to determine which programs or projects could be at risk of foreign interference, theft, and unwanted knowledge transfer. This preliminary analysis supports a risk-targeted approach, aiming to reduce administrative burden and focus limited resources to programs or projects that present a higher level of risk.

While the main objective of this scoping exercise is to determine which programs face a risk due to the involvement of a partner of potential concern, this process may also identify other areas of risk (e.g., risks related to intellectual property, cyber and information technology infrastructure, or physical access) that are contributing to a program or individual project's overall risk profile. Research organizations and funders are encouraged to develop a *Research Security Plan* that is holistic and clearly outlines what additional processes, resources, staffing, or capacity is required to effectively implement a feasible, proportionate, and tailored strategy.

In developing their *Research Security Plan*, organizations should adhere to principles of research security, including but not limited to: maintaining a commitment to open science; allowing for a high degree of adaptability in their research security measures; ensuring accountability as well as responsibility; and ensuring responses are risk-proportionate. Any actions on research security should continue to uphold the principles of research integrity, including academic freedom, institutional autonomy, equity diversity and inclusion, and transparency, among others.

For more information on the principles of research integrity and research security, please consult the publication titled *G7 Common Values and Principles on Research Security and Research Integrity*. By integrating these guiding principles throughout a *Research Security Plan*, a research or funding organization can ensure the integrity and security of the research they fund or conduct.

3.1 Developing and Implementing Your Research Security Plan at the Project Level

Research organizations and funders have different existing internal practices, policies, procedures, and funding evaluation processes. Consequently, this guidance document strives to account for these variations and provides a flexible framework for research organizations and funders to implement information collection, risk assessment, and mitigation measures.

Regardless of the approach taken by a research organization or funder, the *Research Security Plan* should describe how the organization or funder intends to meet these objectives while assessing research projects.

3.1.1 Determining Your Approach

The purpose of any *Research Security Plan* is to outline a set of policies and standard practices for consistently considering and addressing risks when conducting or funding research.

In developing a *Research Security Plan*, there are existing risk management models and resources that can be leveraged to integrate research security into internal processes. Notably, this includes the Government of Canada's existing *Risk Assessment Form* under the *National Security Guidelines for Research Partnerships.*

Alternatively, research organizations or funders can develop their own tools and processes to collect and assess information on risks and identify risk mitigation measures.

A) Risk Assessment Form

The *Risk Assessment Form* was developed to support the implementation of the *National Security Guidelines for Research Partnerships*. It is designed to assess potential risks that research partnerships may pose to Canada's national security and economic prosperity. This form includes a series of prompts specific to research partnerships, the nature of one's research, and identification of mitigation measures.

Research organizations can use any or all of the questions from the *Risk Assessment Form* to assess risks associated to research projects. The *Risk Assessment Form* may be periodically updated in the future to account for evolving security risks and the needs of researchers and funding organizations.

Completing and validating the information in the *Risk Assessment Form* requires utilizing due diligence research methods and tools, many of which are available in the open-source format[2].

B) Standalone Method

Research organizations and funders may also adapt elements of the *Risk Assessment Form* for their own purposes, or develop their own methodology of collecting and assessing information on the risks and mitigation measures associated with research projects and partner organizations. This method should be designed to align with the Government's overall objectives under the *National Security Guidelines for Research Partnerships.* As a reminder, these objectives include:

- Assessing the sensitivity of the research, including whether the research could be at risk or targeted for theft, espionage or foreign interference;
- Assessing the risk level of any partners involved in the research; and
- Identifying effective risk mitigation measures to address identified risks.

Any approach should also be designed to uphold the principles of research integrity, including academic freedom, institutional autonomy, equity diversity and inclusion, and transparency, among other guiding principles.

3.1.2 Operationalizing Your Research Security Plan

A *Research Security Plan* should clearly articulate the organization's planned governance and decision-making processes to integrate research security into its internal operations. For all new processes and structures that are to be implemented, the research organization or funder should clearly specify when these elements are planned to be integrated. This will also help to identify when and where resources should be in place.

Research organizations and funders should provide specific information on ***how*** they intend to implement the following aspects of their research security governance framework:

Conduct and Raise Awareness of Research Security Risks

Research organizations and funders could describe, for example and if applicable:

- What mechanism or measures the research or funding organization will use to increase awareness of research security risks across their community (e.g., conference, workshop, program literature, awareness session, online courses[3], etc.);
- Who from the research or funding organization will develop in-house research security outreach initiatives and informative materials;
- Who from the research or funding organization will carry-out all outreach activities that have been forged in-house;

[2] For more information on open source due diligence, consult the Government of Canada's publication titled Conducting Open Source Due Diligence for Safeguarding Research Partnerships.
[3] Many resources area available through the Safeguarding Your Research Portal, including two short online courses titled Introduction to Research Security and Cyber Security for Researchers .

- When the research or funding organization will disseminate outreach materials; and
- How the research or funding organization will inform their community of new or changing research or funding application requirements.

Collect Information from the Researcher(s) or Applicant(s) on the Sensitivity of the Research, the Partner Organizations, and Associated Risk Mitigations

Research organizations and funders could describe, for example and if applicable:

- How frequently and when the research organization or funder will conduct research security risk assessments;
- How the information will be collected (refer to section 3.1.1 of this document);
- Who from the research or funding organization will be responsible for gathering information related to an applicant's research, partners, and risk mitigation measures; and
- How the research organization or funder will address missing information or incomplete research or funding applications (e.g., if an applicant identifies risks in their research partnership application, but does not provide any mitigation plan).

Assess Risk and Effectiveness of Mitigation Measures

Research organizations and funders could describe, for example and if applicable:

- What internal capacity is available and what external expertise will be outsourced, if required, to assist in assessing risks and mitigation measures;
- Who from the research or funding organization will assess the research security elements of an application (research, partners, mitigation measures), including who from the organization will determine whether additional mitigation measures are warranted;
- How the research or funding organization will periodically review and update their assessment approach to account for changing and emerging risks or threats to research and projects;
- Who from the research or funding organization provides a recommendation to the decision-making body responsible for deciding whether an application/research project should proceed or be funded; and
- What risk threshold will the research or funding organization use to determine if an application poses an unacceptable level of risk.

Make Decisions

Research organizations and funders could describe, for example and if applicable:

- Who from the research or funding organization will approve the funding decisions (what is the internal accountability structure);
- How and where the research or funding organization will document the rationale for each granting decision;
- What factors or criteria will be used to determine a funding decision or if a project proceeds;
- How will the research or funding organization communicate and inform researchers or applicants of funding decisions; and
- How will the research or funding organization address appeals to a funding decision.

Maintain Compliance, Monitoring, and Reporting Practices

Research organizations and funders could describe, for example and if applicable:

- What is the compliance and enforcement approach for holding individuals accountable for upholding the *Research Security* Plan;
- How the research or funding organization will integrate research security terms and conditions into existing and future grant agreements;
- How the research or funding organization's research security plan will be integrated into university policies, contracts, codes of conduct, etc.;
- What tools for promoting and monitoring compliance and the range of enforcement actions are available to the research or funding organization;
- How the research or funding organization will address non-compliance;
- Who from the research or funding organization has the authority to conduct disciplinary measures that address acts of non-compliance;
- Who from the research or funding organization is responsible for recording security incidents/breaches;
- How the research or funding organization will report on the type and number of security incidents/breaches; and
- Who from the research or funding organization is responsible for answering any questions related to research security.

3.2 Developing and Implementing Your Research Security Plan at the Organizational Level

In addition to articulating how a research or funding organization will identify, assess, and mitigate the security risks associated with their research projects and partnerships, these organizations have a responsibility to secure information and research that is being collected from researchers and funding applicants. A *Research Security Plan* at the organization level is intended to bolster the organization's internal operations that will protect against both insider and outsider threats to research security.

3.2.1 Operationalizing Your Research Security Plan

This aspect of a *Research Security Plan* should clearly articulate how the research or funding organization intends to maintain, adjust, or adopt research security considerations into its corporate and risk management strategies.

Research organizations should provide specific information on ***how*** they intend to internally adopt the following security components and considerations:

Maintain Physical Security

Research organizations and funders could describe, for example and if applicable:

- Who will monitor the emergence of internal and external threats that may jeopardize the organization's infrastructure and research security resiliency;

- Who has access to restricted areas of research facilities;
- What types of visitors are or are not allowed into the physical building or research laboratory;
- What are the physical and data access controls that the research or funding organization has in place, including, physical barriers, surveillance, alarms, and mechanisms to detect unauthorized access;
- What are the protection measures in place for equipment owned by the research or funding organization;
- What back-up systems or storage repositories exist; and
- How research and related assets will be safeguarded when personnel are traveling outside of Canada.

Ensure Personnel Suitability and Reliability

Research organizations and funders could describe, for example and if applicable:

- What are their personnel pre-hiring security screening protocols, and ongoing suitability and reliability procedures;
- Who will conduct appropriate reference and security checks;
- How will potential or existing personnel conflicts of interest be identified and addressed; and
- What security training requirements for personnel that are in place or would be developed.

Integrate Information Management and Cyber Security Practices[4]

Research organizations and funders could describe, for example and if applicable:

- How the research or funding organization will classify and determine each asset's level of security;
- How any personal data, research, and information collected from researchers and applicants will be stored;
- Who has access to IP, research, personal data, and any other sensitive information;
- What mechanisms are in place that help maintain the safe storage of IP, research, and personal data;
- How possible cyber security gaps will be identified and assessed[5];
- How the research or funding organization will share or publish their data, research methods, results, etc., with applicants and respective partners; and
- What policies are in place within the research or funding organization to ensure the safe transfer of knowledge and research to involved stakeholders.

[4] Research security plans may link or reference an organization's cyber security plan, if they exist. Another option may be to voluntarily incorporate the cyber security plan into a research security plan.

[5] For more information on cybersecurity practices and considerations, please consult the Government of Canada virtual "CyberSecure Canada eLearning Series".

Adopt Incident and Emergency Response Measures[6]

Research organizations and funders could describe, for example and if applicable:

- What mechanisms are in place to detect unauthorized access to facilities, IP, research, and personal data (i.e., detect physical security breach, cyber incidents, possible loss of intellectual property conflict of interest, etc.);
- How incidents will be reported both internally and externally and to whom;
- How incidents will be responded to in a timely and coordinated manner; and
- What incident investigation procedures are in place.

4. Final Considerations

To summarize, the main objective of a *Research Security Plan* is to lay out a governance framework demonstrating how research organizations and funders intend to identify and assess research that could be at risk or targeted for theft, espionage or foreign interference; and to develop and implement proportionate and feasible risk mitigation measures.

The development and implementation of a *Research Security Plan* will strengthen an organization's existing security framework and help meet objectives that safeguard Canadian research and Canada's national security interests. Furthermore, the use of a *Research Security Plan* will permit research organizations and funders to maintain a high level of transparency among researchers, funding applicants, partners, and the government.

In sum, a *Research Security Plan* is a mechanism that research and funding organizations can use to further develop a culture of research security within their organization, and to raise awareness on the importance of research security among their community. Ultimately, a *Research Security Plan* should demonstrate a research or funding organization's commitment and shared responsibility to safeguarding Canada's research ecosystem through risk-proportionate measures and continual improvement and integration of research security into business processes.

[6] An incident and emergency response plan is a collection of procedures for responding in a timely and effective manner to situations that could impact security of assets and individuals. It should include procedures for incident reporting, incident response, and incident investigations.