U15 Canada

Safeguarding Research in Canada

A Guide for University Policies and Practices

June 2026

This paper will be updated as required by the U15 Canada Research Committee.

June 2026

U15 Canada acknowledges consultations with the Canadian University Council of Chief Information Officers (CUCCIO), whose insights helped inform the cybersecurity and digital infrastructure considerations reflected in this paper.

U15 Canada

Table Of Contents

Executive Summary

Canada's research ecosystem is built on openness, international collaboration, and the global exchange of people and ideas to advance knowledge, develop talent, drive innovation and deliver impact for all Canadians. At the same time, a changing geopolitical and security environment is shaping new risks, including unauthorized knowledge transfer, intellectual property theft, cyber threats, and risks to research infrastructure, data, partnerships, and people.

Canada's leading research universities take the importance of maintaining research security extremely seriously. In recent years, universities have acted proactively to safeguard research, including establishing clear internal policies for the secure conduct of research, strengthening due diligence on research partnerships and establishing dedicated research security offices to advise researchers on evolving threats.

This guide builds on this work to provide leading practices to help Canadian universities safeguard research while preserving the values that underpin secure research: integrity, respect, people, trust, resiliency and compliance. It recognizes that research security is a shared responsibility between universities and government partners.

The guidance is intended to support institutions and researchers in developing their own approaches to research security, building on leading practices at U15 universities. It highlights the importance of clear governance and risk frameworks, consistent and transparent due diligence, engagement with federal, provincial, and territorial governments, coordination across institutional units, cybersecurity and data protection, informed procurement, partnership assessment, communication, training, and campus security.

A central principle is that safeguarding research must be proportionate, inclusive, and evidence-informed. Risk mitigation should not undermine the openness and diversity that make Canadian universities a vibrant and collaborative place to conduct research. As research security risks and requirements continue to evolve, this document is intended to serve as an evergreen resource that will be updated regularly.

About U15 Canada

U15 Canada is an association of fifteen leading research universities across Canada. U15 Canada works to optimize research and innovation policies and programs that advance knowledge, develop highly qualified leaders for all sectors, and mobilize knowledge for the benefit of all Canadians. In this way, U15 Canada seeks to help Canadian universities and partners make a prosperous, sustainable and just future for all.

Introduction

A defining characteristic of Canada's university system is its openness to the world. Global engagement is indispensable to the success of our top research-intensive universities, their competitiveness on the world stage, and their ability to enhance the quality of life of Canadians through learning, discovery, and community service. As stated by the Chief Science Advisor of Canada in describing open science, the practice of sharing data, information tools, and research results while also eliminating barriers to collaboration, accelerates discovery and encourages transparency, scientific integrity and professional accountability.

A second defining characteristic of Canada's leading universities is their commitment to ensuring the responsible conduct of research and research integrity. Over many years, Canadian universities have developed robust policies and practices that guide how research should be conducted throughout the life cycle of each project in keeping with the highest standards of honesty, fairness, trust, accountability, and openness. These university policies and practices operate within the context of federal guidelines such as the Tri-Agency Framework: Responsible Conduct of Research (2021) and the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS 2 (2022), as well as other guidelines, including those on animal care.

This global engagement and commitment to the responsible conduct of research enable Canadian researchers to make cutting-edge breakthroughs as they work in collaboration with others worldwide. It enables our universities to attract and educate many of the world's best students. It enables Canada to recruit outstanding global experts to teach and conduct research. And it ensures that Canadian university students are enriched by engaging with classmates from a wide diversity of backgrounds. Welcoming talent from around the world, regardless of country of origin, is an essential element of Canada's current and future success as an open, inclusive, and prosperous country. Ultimately, the global exchange of ideas is made possible by this global exchange of people.

In recent years, there has been concern that some foreign entities are seeking to exploit and misuse the very openness and inclusivity that drives our success and world-class performance. This concern led to the creation of the Government of Canada-Universities Working Group on Research Security in 2018 in order to advance open and collaborative research in a way that also safeguards research and maximizes benefits to Canadians. Achievements thus far through regular meetings of the Working Group include the development of the National Security Guidelines for Research Partnerships, and the subsequent Government of Canada's Policy on Sensitive Technology Research and Affiliations of Concern (STRAC) that includes the Named Research Organizations (NRO) list and the list of Sensitive Technology Research Areas (STRA) (See Appendix 1.0 for full list).

In keeping with the shared responsibility for research security, in which Canada's national intelligence services keep Canadians informed about research risks**,** institutions have been building on their established policies and practices for supporting the responsible conduct of research by taking the next steps required to safeguard research.

Toward this end, universities have made significant investments in the development of sophisticated risk management frameworks and associated policies and practices, including the management of risk associated with international collaborations, research partnerships and the protection of research data, research results and intellectual property. Additionally, universities and their collaborating partners have invested significantly in the cybersecurity realm to develop national and provincial services to identify, manage and respond to threats to digital assets.

To build on this work, this document provides a collection of suggested institutional guidelines based on leading policies and practices for safeguarding research from the potential risks in global research engagement. The described practices reflect the commitment of universities to collaborate on developing leading policies and practices through research offices, and on accessing shared technologies to help identify, assess, and mitigate threats to research security. The document should be viewed as an evergreen document that will be regularly reviewed for updates, as developments and activities related to safeguarding research evolve.

The following leading practices provide guidelines for institutions to consider in developing their local best practices, given their context.

Values Underpinning the Leading Practices

These values underpin our collective approach to developing leading practices for safeguarding research at Canadian institutions.

1. **Integrity:** as a core principle for researchers and institutions.
2. **Respect:** for academic freedom, open-science and diverse and inclusive university environments.
3. **People:** supporting the research community through clear guidance, training and a culture of inclusion and shared responsibilities.
4. **Trust:** across funders, partners, governments, and universities.
5. **Resilience:** in developing policies and practices to safeguard research and advance research activity.
6. **Compliance:** with all relevant laws, regulations, and ethical standards related to research security.

Principles for Safeguarding Research at Canadian Universities

Suggested leading practices for safeguarding research for the benefit of Canada are guided by the following principles:

1. **Transparency**: Transparent within the institution, with our federal and provincial/territorial governments, and with our broader communities.
2. **Predictability**: Provide predictability for researchers, research administrators, as well as our governments and the larger society.
3. **Engagement and inclusivity**: Engagement across the university, with particular attention towards upholding principles of diversity, equity, and inclusivity.
4. **Protection of researchers, their research and research spaces:** Support researchers in protecting their research from foreign interference, espionage, intellectual property theft or unauthorized knowledge transfer.
5. **Consistency**: Consistency in risk assessment of research projects on national security grounds.
6. **Breadth and depth of perspectives**: Ensure there is broad disciplinary expertise and intricate knowledge of national security and cybersecurity risks leveraged for accurate risk assessment and mitigation.
7. **Shared Responsibility**: Safeguarding research is everybody's responsibility, from the federal government to administrative offices to faculty members.
8. **Innovation and Knowledge Transfer:** Enabling research impact by supporting open, secure, and responsible commercialization and knowledge mobilization.

Suggested Leading Practices for Safeguarding Research at Canada's Universities

1. Governance and Risk Frameworks

Governance and risk assessment frameworks can be used to guide the integration of risk mitigation strategies into existing policies and procedures. They also identify where best practices can be incorporated into each university's strategies to safeguard research.

1.1. Institutional Research Safeguarding

Practice

Develop a university governance and risk framework for safeguarding research that complements federal government guidelines, and, where appropriate, those of provinces/territories. In doing so, institutions should seek to provide to researchers clarity and consistency on the expectations among any government requirements, the National Security Guidelines risk assessment process and other guidelines and/or criteria that are developed by governmental or institutional authorities.

Outcomes

- University researchers are provided with procedures and resources to safeguard their research and adhere to research-security requirements.
- Enhanced transparency, predictability, and equity in the safeguarding research process.
- Strengthened institutional policies and practices on research security.

Best Practice Actions

- When developing the governance and risk framework, it is recommended that universities consult and engage relevant academic and administrative stakeholders and accountable authorities within the university. Toward this end, promising approaches include:
    - Building collaborations that may include representation from key researchers, faculties, departments, centres and institutes and administrative support units, such as campus security, information technology services, global engagement, graduate and postdoctoral studies, commercialization, entrepreneurship, innovation and partnership offices and procurement, to inform the development of institutional practices that are governed by institutional principles, policies and practices.
    - Developing university risk assessment and mitigation approaches for possible adaptation in specific research activities. These could range from actions such as declarations of conflicts of interest to other appropriate means of assessing and forming appropriate partnerships/collaborations, etc.

- Ensure the university benefits from membership in relevant associations such as U15 Canada and Universities Canada to ensure effective communication with federal governments, and where appropriate, provincial-territorial governments.
- Communicate to information technology units the expectations for participation in relevant national and provincial cybersecurity initiatives and services.
- Establish open and frequent communication with Provincial/Territorial and Federal governments (i.e., Innovation, Science and Economic Development Canada (ISED), Public Safety Canada, Tri-Agencies and provincial associations), funding agencies (i.e., MITACS and Genome Canada) and consortia across the sector (i.e., Universities Canada and U15 Canada).

1.2. Government Engagement Strategy

Practice

Engage with governments, when necessary and as appropriate, at both the federal and provincial/territorial levels, to consult on and implement the National Security Guidelines for Research Partnerships, the Policy on Sensitive Technology Research and Affiliations of Concern and other governmental safeguarding research guidelines, regulations, principles and policies.

Outcomes

- Greater harmonization between government and universities on risk mitigation issues, best practices, and information sharing.
- Greater consistency, efficiency and understanding of research partnership and mitigating decisions undertaken in various institutions.
- A more comprehensive understanding regarding the role and application of dual-use or sensitive technologies and export control regulations.
- Facilitate greater sharing of information from government agencies on threat actors, tactics, techniques, risk, vulnerabilities, and trends.
- Greater clarity from federal, provincial and territorial governments on thresholds and risk tolerances.

Best Practice Actions

Work with the Government of Canada's Research Security Center and other agencies within Public Safety Canada, as well as with the provincial/territorial governments, as appropriate, to ensure a common understanding of principles and objectives and emerging national security threats and trends.

- Engage with appropriate provincial/territorial authorities to establish a common understanding of research security frameworks and assessment processes utilized within individual provinces/territories.
- Collaboratively develop and utilize open-source methods and resources for completing risk assessments and risk mitigation plans under the National Security Guidelines for Research Partnerships, the STRAC policy, and other relevant federal or provincial requirements, while collaborating on the sharing of cost-effective tools to assess risk.
- Engage globally with trusted partners to develop common practices and shared understanding.
- Leverage national and provincial/territorial services and act as stewards and advocates of the programs to ensure continued funding that manages risks to the digital security of research.

1.3. Existing Institutional Risk Framework/Policies/Guidelines

Practice

Review existing institutional guidelines or policies to consider where explicit consideration of safeguarding research is acceptable and warranted.

Outcomes

- Establish clear and documented safeguarding research risk mitigation practices and guidelines.

Best Practice Actions

- Leverage existing institutional policies, procedures, and frameworks that can be utilized to safeguard research.
- Identify any gaps or issues relating to appropriately safeguarding research in the context of established policies and practices for the responsible conduct of research and address them to ensure an overall coherent and consistent institutional approach to research management.
- Develop and share risk frameworks, including foreign interference threats to people, information, systems, and assets. For example, risk management frameworks around third-party vendor selection.

1.4. Ground Research Security in the Principles of Equity, Diversity, and Inclusion and Mitigate the Effects of Racial and Ethnic Profiling on the Academic Community

Practice

As part of their initiatives to combat racism and ethnic profiling, institutions have an important role to play in ensuring that efforts to support research security include specific anti-racism and anti-ethnic profiling action to support racialized researchers whose research

programs may be subject to safeguarding research guidelines and practices. To this end, institutions should advocate for, support, and enable inclusive research environments, policies and practices, so that researchers are enabled to pursue appropriate international scientific inquiry which aligns with research security without fear of prejudice, profiling, or persecution.

Outcomes

- Universities offer an enriching and safe climate for all researchers, regardless of their origin or background.
- Universities safeguard research while upholding principles of equity, diversity and anti-racism.

Best Practice Actions

- Identify mechanisms to maintain the spirit of international collaboration while safeguarding international and domestic researchers.
- Ensure research security training and messaging work within an anti-racist and inclusive framework while emphasizing the importance of a secure international and collaborative scientific community.
- Monitor unintended consequences of risk assessments faced by researchers, specifically related to issues pertaining to diversity, equity, inclusion and self-censorship.

2. Due Diligence, Risk Assessment and Management

The activities related to due diligence, risk assessment, and risk management should guide the university in identifying, assessing, and mitigating risk and ensure university stakeholders understand their role in informed decision-making and help guide practices.

2.1. Due Diligence, Risk Assessments and Management Related to Corporate Partners

Practice

Assist researchers in their risk assessments of partners, provide clarification of at-risk activities (e.g., dual-use, sensitive, or strategic technologies), and assist in preparing and actioning risk mitigation plans.

Outcomes

- Researchers and institutions have the tools and training available to develop the expertise required to implement the research security processes required for compliance.
- Commercialization contracts are updated to include standardized language that acknowledges the requirements and processes in place to protect IP and manage research security risks.

- Domestic and International research partners are re-assured of a safeguarded research environment.
- Processes are developed to manage research security issues related to reputational risk.

Best Practice Actions

- Collaborate with researchers to co-develop risk assessment and mitigation strategies. Where desirable and feasible, provide engagement formats of various kinds, including one-on-one, to facilitate better learning outcomes and more robust risk mitigation strategies. Discussions could also facilitate the sharing of best practices of risk assessment, particularly across research teams.
- Provide campus researchers with a clear internal process for discussing research security issues with the research security team.
- Continually monitor unintended consequences of risk assessments faced by researchers, such as a reluctance to pursue funding opportunities.
- Develop approval and audit processes and continuously evaluate due-diligence processes.
- Enact continuous learning and improvement in the development of risk assessments.
- Ensure training, resources, and standards are available to the community.

2.2. Diversify Funding Sources

As the pool of possible research funding sources becomes smaller due to research security regulations and geopolitical tensions, institutions have a role to play in forging new research collaborations that can potentially lead to new funding sources.

Practice

As appropriate, research offices should work with researchers working in sensitive research areas to assist them in diversifying funding sources to ensure compliance with the National Security Guidelines for Research Partnerships.

Outcomes

- Researchers have a diversity of funding partners that support their research ambitions.
- Leading-edge research and innovation are sustainably funded over the long term.
- Institutions continue to draw top talent through funding opportunities.

Best Practice Actions

- Where possible, identify, assess and evaluate alternative funding sources.
- If possible, conduct a mapping exercise of key partner networks to understand institutional and contractual linkages and identify alternative funding sources.

- Advocate for expanded government funding sources for sensitive research.

2.3. Assessing University-Specific Priority Areas

Understanding vulnerabilities will allow prioritization of areas which may require further protection, particularly with respect to cybersecurity, data management and physical infrastructure practices and protocols included under the purview of national and provincial/territorial research security guidelines. Given the inherent complexity and capability required for adequate cybersecurity protection, institutions should advocate that best practices are followed, which will entail that new funding be allotted to build capacity and upgrade existing systems.

Practice

Ensure university stakeholders, including Information Technology teams, are aware of the Government of Canada's Sensitive Technology Research Areas (STRA) list, where particular research areas are identified as vulnerable to foreign exploitation, as well as other national and provincial/territorial guidelines and policies related to safe and responsible cybersecurity, data management and physical infrastructure requirements.

Outcomes

- Research security teams look for opportunities to provide educational outreach on new and changing requirements related to the National Security Guidelines for Research Partnerships, the STRAC policy, sanction regimes, export controls and controlled goods regimes, and/or criteria developed by other governmental or institutional authorities.
- Researchers are more aware of current threats and how to protect their resources.

Best Practice Actions

- In collaboration with other university partners, such as Information Technology services, where possible, consult researchers and managers of research facilities to check for vulnerabilities and to identify and provide mitigation strategies around security gaps in order to build institutional resilience.
- In collaboration with other campus partners, such as Information Technology services, and as appropriate, engage with researchers and managers working in sensitive research areas, or high-risk partnerships, and provide educational outreach about potential threats and the implementation of risk mitigation plans.

2.4. Institutional International Partnerships

Practice

Work with international offices, where relevant, to align formal institutional international partnerships in sensitive research areas with safeguarding research principles, taking into account the Government of Canada's Named Research Organizations (NRO) list, as well as those entities under sanction by the Government of Canada and any other sanctions regimes, export controls and controlled goods regimes, and/or other provincial/territorial policies and

guidelines. For example: agreements signed with foreign governments named on the Government of Canada sanctions list; and taking into account commercial or public entities that are banned under existing Government of Canada legislation or administration sanctions, such as those in the Telecom and Artificial Intelligence sectors.

Outcomes

- Researchers are more aware of potential international partnership risks.
- University staff are better equipped to understand, undertake risk assessments and develop risk mitigation strategies related to sensitive research involved with international partnerships.

Best Practice Actions

- Institutions can align and coordinate with relevant security guidelines of trusted partners, such as export controls and cyber-security standards, to facilitate compliance regulations. This coordination will allow universities to avoid bearing unnecessary risk associated with cyber- breaches and ensure regulatory compliance.
- International engagements in areas of sensitive research should be consistent with the Government of Canada's NRO list, sanctions imposed by the Government of Canada, and Provincial/Territorial governments.
- Develop risk assessment and mitigation strategies for international institutional partnerships in areas of sensitive research.
- Progressively develop processes for conducting internal risk assessments, where possible, of international institutional MOUs and for screening various new international partnerships in sensitive research areas.
- Provide useful and relevant information to researchers and units that guides international engagements in sensitive research areas.
- Engage with other Canadian institutions through existing network organizations to share best practices, perspectives, and processes on international partnerships and support consistency in approaches across the sector.
- Continue to strengthen internal links among institutional units which engage in and support international partnerships, including offices that deal with research and international activities.

2.5. Procurement – Risk / Benefit Analysis

Organizational supply chains need critical research security considerations. They are often mechanisms through which theft, interference with, or unauthorized transfer of, knowledge or data can occur. Assessing and mitigating the risk that potential and existing vendors pose to critical institutional infrastructure and services should be a key component of campus research security programs.

Practice

Procurement processes should apply the appropriate Government of Canada's recommendations and tools related to Integrating Security Considerations into Procurement of Research Goods and Services.

Outcomes

- A clear and transparent process for vetting potential vendors who supply products and services to the institution can expedite better business outcomes.

Best Practice Actions

- Institutions proactively develop effective guidelines and policies for product and service procurement that align with federal and provincial/territorial research security guidelines.
- Through educational outreach, research security teams can inform and support applicants and grant holders about restrictions.

3. Communication, Education and Knowledge Sharing

Safeguarding research is a sensitive topic. Universities should be proactive and thoughtful about their communications at all levels within their organizations to develop resilience and avoid undue negative impacts on any of their members.

3.1. Website as a Resource Hub for Institutional Activities and Supports

Practice

Build a single, publicly accessible portal for the institution, such as a website, which brings together supports and services to the broader community regarding research security issues, principles, and up-to-date guidelines.

Outcomes

- Through targeted educational outreach around the website, university community members will be better informed about changing requirements.
- University community members are provided with consistent and transparent information.

Best Practice Actions

Develop and include training materials that focus on safeguarding research and cybersecurity/digital-hygiene best practices.

- Regularly update the portal with relevant information, such as risk mitigation forms, event dates for workshops, information sessions, and training.
- Seek feedback from the community to continually improve the portal.

3.2. Learnings from other Canadian organizations

Practice

Active engagement with partners (regionally, provincially/territorially, and across Canada), such as through peer-institution working groups, communities-of-practice, U15 Canada, and Universities Canada, on safeguarding research best practices, to enable the sharing of best practices and approaches.

Outcomes

- Greater knowledge and faster implementation of best practices at institutions across regions, provinces and Canada, relevant to the context of the institution.
- Increased collaboration on strategies to anticipate and mitigate risks related to the safeguarding of research.
- Amplification of the key messaging of the institution to achieve greater impact on best practices across the institution.
- Stronger interpersonal relationships between research security practitioners and the Government of Canada and provincial/territorial staff, where appropriate.

Best Practice Actions

- Engage with other provincial/territorial institutions to bring together staff leading safeguarding research work, such as research security officers and cybersecurity specialists, to share protocols and practices.
- Develop formal and informal networking groups within provinces and across the country, such as expert briefing series, working groups and communities-of-practice amongst research security officers to enable understanding of various approaches and harmonization where possible.
- Continually refine safeguarding research principles based on useful common practices.
- Align institutional safeguarding practices with sensitive research data classification frameworks.
- Leverage federally funded cybersecurity services and programs through CANARIE and NREN partners (eg. CanSSOC Threat Feed, National Cybersecurity Assessment, Cybersecurity Initiatives Program, regional SOCs), CIRA (e.g. DNS firewall) and the Digital Research Alliance of Canada (eg. Cloud Connect) and CUCCIO (Benchmarking).

3.3. Learnings from other jurisdictions

Practice

Engage with international partners on best safeguarding research practices, leading to greater awareness of international best practices.

Outcomes

- Greater understanding of practices across key international partners.
- The creation of a global network of trust and best practice sharing for learning and compliance across other jurisdictions.
- This network could also function as a facilitator for awareness around international funding opportunity research security guidelines.

Best Practice Actions

- Through relevant consortia such as U15 Canada and Universities Canada, engage with university counterparts in trusted partners to understand their protocols and current practices.
- Continually refine safeguarding research principles based on useful common practices.

3.4. Host regular major events to hear community-wide views

Practice

Invite key stakeholders (i.e., provincial/territorial and federal officials, funding agencies, researchers, research security experts) to discuss issues relating to safeguarding research and help raise our level of common and mutual understanding.

Outcomes

- An enhanced shared and mutual understanding of the key issues as the landscape evolves.

Best Practice Actions

- Engage with researchers, research security experts, cybersecurity experts, peer-institutions, and government to convene meetings and workshops.
- Convene regular opportunities for networking.

4. Network and Device Security

A university's vulnerability to cyber-attacks is influenced by its range of activities, size, and complexity. With the shift toward digital in research, education, and communication, there is an increased need for attention to cybersecurity. Practices and outcomes should be continually kept up to date and revised as necessary to reflect changing vulnerabilities. For institutions to operationalize the full requirements that will ensure that these practices and outcomes are kept up to date and modernized, additional funding will be necessary.

Practice

While considering institutional ability, appropriate university bodies should progressively monitor institutional networks and devices in alignment with existing standards in these

domains to ensure they are secure and reduce the probability of cyberattacks, hacking, and network manipulation.

Outcomes

- Reduced probability of cyberattacks, hacking, and network manipulation.
- Alignment and compliance with international security standards. This coordination will allow universities to avoid bearing unnecessary risk associated with cyber- breaches

Best Practice Actions

- Follow existing security frameworks, such as ISTG-33, the Government of Canada's national standards for cyber-security, and relevant international cybersecurity frameworks such as the National Institute of Standards and Technology (NIST), while developing guidance for new developments.
- Promote cybersecurity training uptake for researchers given its critical role.
- Support appropriate campus groups to enable greater security of research computing and storage assets on appropriate infrastructure.

5. Research Security and Campus Security Services

Understanding vulnerabilities of research spaces and laboratories which operate with federal and provincial funding is important. Allowing researchers and other staff to understand which areas may require further protections, particularly with respect to cybersecurity and the strengthening of data management and protocols, is critical. This includes existing university physical and digital security resources. Institutional costs to protect physical and digital campus infrastructure and security systems are high and necessitate both education and guidance from research security offices and further external financial support.

Practice

Given individual institutional ability, utilize a whole institution approach to progressively mobilize university partners to understand vulnerabilities and assess and mitigate risks to research spaces and sensitive research projects within existing frameworks for grant applications, such as controlled goods planning.

Outcomes

- Greater understanding of existing campus security mechanisms may lead to harmonization between research offices, campus security teams, and university management on risk mitigation strategies.
- A more comprehensive understanding regarding the role of campus security and IT teams in the delivery of the research security mandate within universities.
- Canadian institutions can align and coordinate with international research security standards to avoid unnecessary risk associated with cyber-security.

- Increased guidance and support for researchers to protect them from foreign interference and transnational repression.

Best Practice Actions

- Consult with researchers to understand current security gaps within laboratories, research spaces and areas of vulnerability and eliminate risks to build institutional resilience.
- Engage with research leaders, safety offices, plant and facility operations, information technology and campus security services to:
    - Assess the requirement for potential additional security measures in sensitive labs and research spaces.
    - Construct mitigation strategies for the protection of sensitive research areas.
- Expand access to resources, guidance, and clear reporting pathways related to foreign interference, intimidation, harassment, and transnational repression, including practical direction for researchers, students, trainees, and staff on how to seek support, document concerns, and respond when they feel unsafe, pressured, or targeted by a foreign entity.

Appendix 1.0 – Research Security Policies and Guidelines

Government of Canada

Canadian Centre for Cyber Security: Information and academia

Canada Foundation for Innovation Guidance on Research Security

Conducting Open Source Due Diligence for Safeguarding Research Partnerships

CSIS - Protect your research: Alberta

CSIS - Protect your research: British Columbia

CSIS - Protect your research: Manitoba

CSIS - Protect your research: Newfoundland and Labrador

CSIS - Protect your research: New Brunswick

CSIS - Protect Your Research: Northwest Territories

CSIS - Protect your research: Nova Scotia

CSIS - Protect Your Research: Nunavut

CSIS - Protect your research: Ontario

CSIS - Protect your research: Prince Edward Island

CSIS - Protect your research: Quebec

CSIS - Protect your research: Saskatchewan

CSIS - Protect Your Research - Yukon

Integrating Security Considerations into Procurement of Research Goods and Services

National Security Guidelines for Research Partnerships

Policy for Sensitive Technology Research and Affiliations of Concern (STRAC)

Sensitive Technology Research Areas (STRA)

Named Research Organizations (NRO)

Tri-agency guidance on research security

Provincial Guidelines

Research Security Guidelines for Ontario Research Funding Programs

International Research Partnerships Framework for Saskatchewan