A Shared Commitment by Universities to Protect Ontario's Research

Council of Ontario Universities

June 23, 2023

Table of Contents

Introduction

Global engagement is indispensable to the success of our universities, their competitiveness on the world stage, and their ability to enhance the quality of life of Ontarians and Canadians through learning, discovery, and community service. While openness, collaboration, equity, diversity and inclusion are critical to discovery and innovation, Ontario's universities recognize that vigilance is critical to preventing loss of opportunities, as well as to ensuring research conducted on campuses is not misused and continues to be converted into tangible benefits and economic prosperity for Ontario and Canada.

With a shared goal to safeguard Ontario and Canada's research ecosystem through openness and responsible conduct of research, Ontario's universities are partnering with all levels of government – as well as allies through the G7 research security and integrity working group – to ensure research is secure. Universities have robust policies and practices on research conduct, keeping with the highest standards of honesty, fairness, trust, accountability and openness. These 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.

In today's rapidly shifting geo-political environment, safeguarding research will continue to be a priority for universities across the province, as university research offices continue to take reasonable and risk-based measures to safeguard investments in research.

In fact, Ontario universities have been leaders, in collaboration with the Province of Ontario and Government of Canada, in establishing a national security framework for university research and have supported discussions with the Government-Universities Working Group on Research Security.

Universities will continue to follow guidelines set by government agencies and funders, protecting research for the benefit of Ontario and Canada. Universities work to identify and manage the risks associated with areas of research these agencies consider to be of national strategic importance.

Enhancing the security and integrity of universities' research enterprise will help protect research data and intellectual property and promote safe partnerships.

The document should be viewed as an evergreen document that will be annually reviewed for updates, as developments and activities related to safeguarding research evolve.

These values underpin our collective approach to safeguarding research leading practices at Ontario institutions.

1. **Integrity:** as a core principle for researchers and institutions

2. **Respect:** for academic freedom, open-science and diverse and inclusive campus environments

3. **Trust:** across funders, partners, governments, and universities

4. **Resilience:** in developing policies and practices to safeguard research and advance research activity

5. **Compliance:** with all relevant laws, regulations, and ethical standards related to research security.

Safeguarding Research Principles for Ontario Universities

Institutions should collaborate on developing best practices *through research offices and on accessing shared technologies to help identify, assess and mitigate threats to innovation and research security.*

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 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.

Leading Practices to Safeguarding Research at Ontario's Universities

1. Governance and Risk Frameworks

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

1.1. Institutional Research Safeguarding within the Responsible Conduct of Research

Practice

Develop an institutional governance and risk framework for safeguarding research that aligns with Ontario and complements federal government guidelines. 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 supported in understanding services to safeguard and in following granting agency and other sponsor's procedures.
- Greater transparency, predictability, and equity in the safeguarding research process.
- Strengthened institutional policies and practices on research security.

Actions

- When developing the governance and risk framework, universities consult and engage relevant academic and administrative stakeholders and accountable authorities in the university. Toward this end, promising approaches include:

  o Build an interconnected team to support safeguarding research that would 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.

  o Developing institutional 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 establishes benefits from membership in relevant associations such as Council of Ontario Universities, U15 and Universities Canada to ensure effective communication with Provincial and Federal governments.

- Ensure the university establishes open and frequent communication with Provincial 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., Council of Ontario Universities, Universities Canada and U15).

1.2.   Government Engagement Strategy

Practice

Engage with The Government of Ontario and the federal government to consult on and implement the National Security Guidelines for Research Partnerships and other governmental safeguarding research guidelines, regulations, principles and policies.

Outcomes

- Greater harmonization between government and universities in Ontario on risk mitigation issues, best practices, and information sharing.
- Greater consistency, efficiency and understanding of research partnership and mitigating decisions across all in various institutions.
- More comprehensive understanding regarding the role and application of dual-use or sensitive technologies and export control regulations.

Actions

- Work with the Province of Ontario, the Government of Canada's Research Security Center and other agencies within Public Safety Canada to ensure common understanding of principles and objectives and emerging national security threats and trends.

- Engage with the Ministry of Colleges and Universities and the Ministry of the Solicitor General and other appropriate authorities in Ontario to establish a common understanding of the procedures outlined in the National Security Guidelines for Research Partnerships and other relevant federal or provincial requirements.

- 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 and other relevant federal or provincial requirements; collaborate on the sharing of cost-effective tools to assess risk.

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

- An understanding of how safeguarding research policies and practices fit within the overall conduct of responsible research.

Actions

- Identify any gaps or issues relating to 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 risk frameworks for managing risks to research, including foreign interference threats to people, information, systems, and assets.

- Ensure institutional guidelines, practices, or policies set out responsibilities, obligations, expected conduct, and consequences.

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 and the support of racialized and researchers.

Advocate for and support inclusive research environments, policies and practices, so that researchers are enabled to pursue appropriate international scientific inquiry without fear of prejudice, profiling, or persecution.

Outcomes

- Universities offer an enriching and safe climate for all researchers.
- International and domestic students feel welcomed in their pursuit of their studies in Canada and do not have to fear reprisal at home or abroad.
- Universities safeguard research while upholding principles of equity, diversity and anti-racism.

Actions

- Identify mechanisms to maintain the spirit of international collaboration, while safeguarding foreign and domestic researchers.

- Be vigilant that 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.

2.   Due Diligence, Risk Assessment and Management

The activities related to due diligence, risk assessment, and risk management 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

Provide assistance to 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 are well supported in the development of risk assessments and mitigation.
- Awareness of research security issues related to the commercialization processes and protecting researchers' intellectual property.
- International research partners are reassured of a safeguarded research environment.
- Professional reputations of the researcher and the institution are upheld.

Actions

- Conduct discussions with researchers to collaboratively develop risk assessments 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 with affected researchers could also facilitate sharing of best practices of risk assessment, particularly across research teams.

- Provide a clear reporting framework for possible foreign interference incidents.

- Continually monitor unintended consequences of risk assessments faced by researchers, such as a reluctance to pursue funding opportunities, with special attention to issues related to diversity, equity, inclusion and self-censorship.

- Develop risk mitigation strategies to support safeguarding the results, methodologies, and data as products of research at the institution within an open science context.

- Develop approval, audit, and continuous evaluation of due diligence processes.

- Enact continuous learning and improvement in the processes of risk assessments.

2.2. Mapping Key Partnership Networks and Supporting Alternative Funding Sources

Practice

When appropriate, research offices should work with researchers to diversify funding sources, including through government support, especially for those working in sensitive research areas that are affected by the national security guidelines.

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.

Actions

- Assess and evaluate alternative funding sources.

- 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 protections, particularly with respect to cybersecurity and the strengthening of data management protocols.

Practice

Ensure your institution is aware of the sensitive areas of science and technology identified by government that are potentially vulnerable to foreign exploitation.

Outcomes

- Institutional infrastructure and resources are better protected.
- Researchers are more aware of current threats and how to protect their resources.

Actions

- Conduct an analysis of sensitive research activities to identify priority areas and potential vulnerabilities and partners that render them sensitive areas.

- Consult with researchers and managers of research facilities to check for vulnerabilities and to identify and eliminate security gaps to build institutional resilience.

- Engage with information technology services and researchers to construct mitigation strategies for critical areas.

- Engage with researchers and managers working in sensitive research areas or higher risk partnerships 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 list of prohibited entities that pose a risk to national security.

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.

Actions

- International engagements in areas of sensitive research should be consistent with the Government of Canada's list of prohibited entities that pose a risk to national security in sensitive areas of technology, rendering them vulnerable to research threats.

- Develop risk assessment and mitigation strategies for international institutional partnerships in areas of sensitive research.

- Develop processes for conducting internal risk assessments 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.

- Develop criteria and training for the consideration of current and potential international partnerships in sensitive research areas.

- Engage with Ontario institutions 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 international partnerships, including offices that deal with research and international activities.

2.5. Procurement – Risk / Benefit Analysis in support of U.S. collaborations

The United States' *John S. McCain National Defense Authorization Act* Section 889(a)(b), public law 115-232, impact current and future U.S. federally funded research grants and contracts.

Section 889(a)(1)(B) prohibits executive agencies from entering into, or extending or renewing, a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, on or after August 13, 2020, unless an exception applies, or a waiver is granted.

If an institution has *any* equipment that is banned, it will prohibit researchers from applying for U.S. federal contracts.

Practice

Institutions to conduct a risk/benefit analysis of potential responses by the institution to the McCain Act to best support researchers.

Outcomes

- A well-developed institutional strategy to address the provisions of the McCain Act

Actions

- Inform and support applicants and grant holders about restrictions.

- Develop processes with procurement, research finance, and research legal counsel to ensure continued compliance with the McCain Act and appropriate language in service contracts.

- Conduct a risk/benefit analysis of potential institutional responses to the McCain Act and develop a response with a researcher focused solution.

- Engage with U.S. partners through relevant consortia such as, Council of Ontario Universities, U15 and Universities Canada to monitor and better understand emerging requirements.

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 ensure a culture of 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, that brings together supports and services to the broader community on how to understand safeguarding research issues, safeguarding research principles and up-to-date guidelines.

Outcomes

- University community members better understand safeguarding research.
- University community members are updated regularly as guidelines change.
- University community members are provided with consistent and transparent information.

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 provincial organizations

Practice

Engagement with provincial partners on best safeguarding research practices, leading to greater harmonization of best practices and approaches across Ontario.

Outcomes

- Greater harmonization, knowledge and faster implementation of best practices across Ontario institutions.
- Greater knowledge and faster implementation of best practices.
- 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.

Actions

- Engage with other provincial institutions to bring together staff leading safeguarding research work, such as research security officers, to share protocols and practices.

- Develop formal and informal networking groups within the province such as expert briefing series, working groups and communities-of-practices amongst research security officers to enable understanding of approaches and harmonization.

- Continually refine safeguarding research principles based on useful common practices.

3.3. Learnings from other jurisdictions

Practice

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

Outcomes

- Greater harmonization of practices across key international partners.
- The creation of a global network of trust and best practice sharing.

Actions

- Through relevant consortia, such as Council of Ontario Universities, engage with university counterparts in peer-countries and peer-institutions 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., Ontario 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.

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 their 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.

Practice

Continually monitor institution networks and devices to ensure they are secure and reduce the probability of cyberattacks, hacking, and network manipulation.

Outcomes

- Reduced probability of cyberattacks, hacking, and network manipulation.

Actions

- Develop guidance for the secure use of portable storage devices.

- Make cybersecurity training available for all researchers and promote uptake.

- Support greater security of research computing and storage assets on appropriate infrastructure.

- Consider implementing a travel device loaner program, particularly for travel to higher-risk countries.

5. Research Security and Campus Security Services

Understanding vulnerabilities of research spaces and laboratories 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. This includes an understanding of on-campus physical and digital security resources.

Practice

Utilize a whole institution approach by mobilizing campus partners to understand vulnerabilities and assess and mitigate risks to research spaces.

Outcomes

- Greater understanding and cooperation may lead to harmonization between research offices, campus security teams, and university management on risk mitigation strategies.
- More comprehensive understanding regarding the role of campus security and IT teams in the delivery of Research Security mandate within universities.
- Enhanced protection of research facilities, research spaces and laboratories.

Actions

- Conduct an analysis of research premises to identify priority areas and potential vulnerabilities within research spaces and IT systems.

- 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 operations, information technology and campus security services campus security teams to:

  - Establish efficient access control measures to research facilities, research spaces and laboratories in areas related to sensitive research.

  - Assess the requirement for potential additional security measures in sensitive labs and research spaces.

  - Construct mitigation strategies for the protection of sensitive research areas.