COUNCIL OF ONTARIO UNIVERSITIES

A Shared Commitment by Universities to Protect Ontario's Research

June 2025

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 and intellectual property, 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 the research ecosystems of Ontario and Canada 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 our 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 geopolitical environment, research security 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. Ontario universities have been leaders, in collaboration with the Province of Ontario and the Government of Canada, in establishing the National Security Guidelines for Research Partnerships 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 to ensure valuable research is protected for the benefit of Ontarians and Canadians. Universities will work to identify and manage the risks associated with areas of research that 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 collection of visionary guiding principles and operational best practices in this document stems from the collective perspective of senior research leaders and research security practitioners in Ontario's higher education sector.

This perspective identifies that safeguarding research includes ensuring that researchers are equipped with the knowledge and support to adhere to national and provincial security requirements, and relevant internal institutional polices. Additionally, researchers should feel safe pursuing their research programs as these requirements shift. In this context researchers refer to faculty, staff and students conducting research.

The following leading practices offer guidelines for institutions to consider in developing their local best practices as suits their organizational needs and context.

Beyond the provision of leading practices for institutions to consider in operationalizing research security using a risk-based approach within their own institutional context, this document affirms that institutional implementation of such requirements requires extensive capability and resources to achieve broader objectives.

The document will be updated annually to ensure ongoing best practices are to keep pace with the rapidly changing research security landscape.

RESEARCH SECURITY VALUES AND PRINCIPLES FOR ONTARIO'S UNIVERSITIES

Values

These values underpin our collective approach to research security leading practices at Ontario's universities.

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.

Principles

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**: Ensure guidelines are transparent within the institution, with our federal and provincial/territorial governments, with our funding agencies, and with our broader communities.
2. **Predictability**: Provide predictability for researchers and research administrators, as well as our governments and the larger society.
3. **Engagement and inclusivity**: Engage researchers across the university in research security education, with particular attention towards upholding principles of equity, diversity and inclusivity.
4. **Protection of researchers, their research and research spaces**: Support all campus researchers in protecting their research from foreign interference, espionage, intellectual property theft or unauthorized knowledge transfer.
5. **Consistency**: Consistently provide assessments 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**: Share the responsibility of research security across all organizational groups, from the federal government to administrative offices to researchers.

LEADING PRACTICES FOR RESEARCH SECURITY 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. These frameworks also identify where best practices can be incorporated into each university's strategies to safeguard research.

Institutional Research Safeguarding Practice

Develop individual institutional governance and risk frameworks for research security that align with Ontario, while complementing the federal government guidelines. In doing so, institutions should seek to provide clarity and consistency to researchers on the expectations among government requirements, such as the Research Security Guidelines for Ontario Research Funding Programs, the National Security Guidelines for Research Partnerships, the Policy for Sensitive Technology Research and Affiliations of Concern (STRAC), sanction regimes, export controls, and controlled goods regimes, and/or criteria developed by other governmental or institutional authorities. In addition, these frameworks should address requirements that researchers at Canadian institutions may be subject to arising from inter-provincial schemes and international funding agency requirements.

Outcomes

- University researchers are supported in understanding services to research security and in following the procedures of granting agencies and other sponsors.
- Enhanced transparency, predictability, and equity in the research security process.
- Strengthened institutional policies and practices on research security.

Best Practice Actions

- When developing the governance and risk framework, universities consult and engage relevant researchers, academic and administrative stakeholders, and accountable authorities within the university.
- Build an interconnected team to support research security. This includes representation from key researchers, faculties, departments, centres/institutes, and administrative support units, such as equity, diversity, and inclusion (EDI) offices, campus security, information technology services, global engagement, graduate and postdoctoral studies, commercialization, entrepreneurship, innovation and partnership offices, and finance and procurement.
- This network of expertise should be used to inform the development of institutional practices that are governed by institutional principles, policies and practices.
- Develop institutional risk assessment and mitigation approaches for possible adaptation in specific research activities. These approaches could range from actions such as declarations of conflicts of interest or commitment to other appropriate means of assessing and forming appropriate partnerships/collaborations, etc.
- Ensure the university engages with relevant associations such as the Council of Ontario Universities and Universities Canada.
- As needed, universities help to facilitate effective and open communication with provincial (i.e., Ministry of Colleges, Universities, Research Excellence and Security (MCURES), Ministry of the Solicitor General) and federal government agencies (i.e., Innovation, Science and Economic Development Canada (ISED), Public Safety Canada), and funding agencies (i.e., tri-agencies, MITACS, and Genome Canada).

Government Engagement Strategy

Practice

Engage with the Ontario provincial government and the federal government to consult on and implement the Research Security Guidelines for Ontario Research Funding Programs, the National Security Guidelines for Research Partnerships, the STRAC policy, and other governmental research security guidelines, regulations, principles, and policies.

Outcomes

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

Best Practice Actions

- Work with the provincial government, the Government of Canada's Research Security Center, and other branches of Public Safety Canada to ensure a common understanding of principles and objectives and emerging national security threats and trends.
- Engage with MCURES, the Ministry of the Solicitor General, and other authorities in Ontario to establish a common understanding of the procedures outlined in Research Security Guidelines for Ontario Research Funding Programs, the National Security Guidelines for Research Partnerships, the STRAC policy, Government of Canada sanctions and export control regulations, and other policies and guidelines.
- Collaboratively develop and utilize open-source methods and resources for completing risk assessments and risk mitigation plans under the Research Security Guidelines for Ontario Research Funding Programs, National Security Guidelines for Research Partnerships, the STRAC policy, and other relevant federal or provincial requirements.
- Collaborate provincially and nationally on the sharing of cost-effective tools and robust processes to assess risk.

Existing Institutional Risk Frameworks/Policies/Guidelines

Practice

Review and update the existing institutional guidelines and policies to consider where explicit consideration of research security is acceptable and warranted.

Outcomes

- Establishment of clear and documented risk mitigation practices and guidelines around safeguarding research policies.

Best Practice Actions

- Identify and address gaps or issues related to research security in the context of established institutional policies and practices.
- Develop and share risk management and best practice-related mitigation frameworks for research security, including foreign interference threats to people, information, systems, and assets. For example, risk management frameworks around third-party vendor selection.
- Ensure institutional guidelines, practices, and policies clearly detail the responsibilities and obligations that institutions and researchers hold in relation to national and provincial research security provisions.

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

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 research security guidelines and policies.

Practice

Advocate for, support and enable inclusive research environments, policies, and practices, so that researchers are empowered to pursue international scientific inquiry, which aligns with research security frameworks without fear of prejudice, profiling, or persecution.

Outcomes

- Universities offer an enriching and safe climate for all researchers.
- International and domestic researchers feel welcomed to pursue their careers and studies in Canada and do not fear reprisal at home or abroad.
- Universities safeguard research while upholding and enabling principles of equity, diversity and anti-racism. Work with the provincial government, the Government of Canada's Research Security Center, and other branches of Public Safety Canada to ensure a common understanding of principles and objectives and emerging national security threats and trends.

Best Practice Actions

- Identify mechanisms to maintain the spirit of international collaboration while safeguarding international and domestic researchers.
- Be vigilant that research security training and messaging incorporate an anti-racist framework that also emphasizes a secure and collaborative international and collaborative scientific community.
- Actively engage in initiatives that promote anti-racism.

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 ensuring university researchers understand their role in informed decision making while helping to guide practices.

Due Diligence, Risk Assessment and Management Related to Corporate Partners

Practice

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

Outcomes

- Researchers and institutions have the tools, training, and expertise required to implement the research security processes required for compliance at the federal and provincial levels.
- Commercialization contracts are updated to include standardized language that acknowledges the requirements and processes in place to protect intellectual property and manage research security risks.
- Domestic and international research partners are reassured of a safeguarded research environment via updated contacts and/or agreements.
- Processes are developed to manage research security issues related to reputational risks.
- The long-term economic security and interests of Ontario are protected against research security risks that could result in the loss or misuse of publicly funded knowledge.

Best Practice Actions

- Collaborate with researchers to co-develop risk assessments and mitigation strategies. Where appropriate, provide various engagement formats, including one-on-one meetings, to facilitate better learning outcomes and more robust risk mitigation strategies.
- Facilitate sharing risk mitigation best practices, particularly across research teams.
- Provide campus researchers with a clear internal process for discussing research security issues with the research security team.
- Continually monitor and develop best practices for addressing unintended consequences of risk assessments faced by researchers. These may include reluctance to pursue funding opportunities in sensitive research areas, or reluctance to attract/hire talent from certain ethnic backgrounds.
- 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.

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 collaborate with researchers working in sensitive research areas to assist them in diversifying funding sources away from those falling under the purview of the National Security Guidelines for Research Partnerships.

Outcomes

- Researchers have a diversity of funding partners that can support their research ambitions.
- Leading-edge research and innovation can be sustainably funded through the long-term development of alternative funding sources not under the purview of the National Security Guidelines for Research Partnerships.
- Institutions can continue to draw top talent through diversified funding opportunities.

Best Practice Actions

- Where possible, assess and evaluate alternative sources of funding.
- If possible, conduct a mapping exercise of key partner networks within research areas to seek alternative sources of funding from partners not subject to the research security guidelines.

Assessing University-Specific Priority Areas

Understanding vulnerabilities will allow prioritization of areas which may require further protection, particularly with respect to safe and responsible cybersecurity, data management and physical infrastructure practices and protocols included under the purview of national and provincial 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 that university campus 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 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 Research Security Guidelines for Ontario Research Funding Programs, 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 aware of current risks and how to protect their information, data and resources.

Best Practice Actions

- In collaboration with other campus 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 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.

Institutional International Partnerships

Work with international offices, where relevant, to align formal institutional international partnerships in sensitive research areas with research security principles, taking into account the Government of Canada's Named Research Organizations (NRO) list of prohibited entities, 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 policies and guidelines outlined by the provincial government. For example: Research Security Guidelines for Ontario Research Funding Programs and MCURES disclosure requirements related to actively funded research agreement inventory with any Named Research Organizations (NROs); agreements signed with foreign governments named on the Government of Canada sanctions list; and commercial or public entities that are banned under the existing Government of Canada legislation or administration sanction, 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 and undertake risk assessments and develop risk mitigation strategies related to sensitive research.

Best Practice Actions

- Ontario institutions can align and coordinate with relevant security guidelines of our Allies, such as export controls and cybersecurity 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 sensitive research areas should be consistent with the Government of Canada's Named Research Organizations (NRO) list of prohibited entities that pose a risk to national security in sensitive areas of technology, as well as with the sanctions imposed by the Government of Canada.
- Develop risk assessment and mitigation strategies for international institutional partnerships in sensitive research areas.
- Progressively develop processes for conducting internal risk assessments of international institutional Memorandum of Understandings and

for screening new international partnerships in sensitive research areas.

- Provide useful and relevant information to researchers and units to guide international engagements in sensitive research areas.
- Through existing network organizations, engage with institutions in Ontario and throughout Canada, to share best practices, perspectives, and processes on international partnerships and support and enable 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.

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 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

Research security is a sensitive topic. Universities should be proactive and thoughtful about their communications within their organizations to ensure a culture of resilience and to avoid undue negative impacts on any of their researchers.

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 research security 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.

Learnings From Other Provincial and Federal Organizations

Practice

Engagement with provincial and federal partners on research security best practices, leading to greater harmonization of optimal practices and approaches across Ontario and the country.

Outcomes

- Greater harmonization, knowledge and faster implementation of best practices across Ontario and Canadian institutions.
- 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 Government of Canada staff where appropriate.

Best Practice Actions

- Engage with other provincial and federal institutions to bring together staff leading research security work, such as research security officers, to share protocols and practices.
- Develop formal and informal networking groups within the province and country, such as expert briefing series, working groups and communities – practice amongst research security officers to enable understanding of approaches and harmonization.
- Continually refine research security principles based on useful common practices.

Learnings From Other Jurisdictions

Practice

Engage with international partners on best research security 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 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 the Council of Ontario Universities, and like-minded G7 partners, engage with university counterparts in peer institutions and peer countries to understand their protocols and current practices.
- Continually refine research security principles based on useful common practices

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 research security 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 the government to convene meetings and workshops.
- Convene regular opportunities for networking and case study review.

4. Consider Network and Device Security

A university's vulnerability to cyberattacks 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. 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

Given individual institutional ability, appropriate campus 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.
- Align and comply 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 the National Institute of Standards and Technology (NIST) cybersecurity framework and develop guidance for new developments.
- Make cybersecurity training available for all researchers and promote uptake.
- Support appropriate campus groups to enable greater security of research computing and storage assets on the appropriate infrastructure.

5. Research Security and Campus Security Systems

Understanding the vulnerabilities of campus research spaces and laboratories which operate with federal or provincial funds 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 practices and protocols, is critical. This includes existing on-campus 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

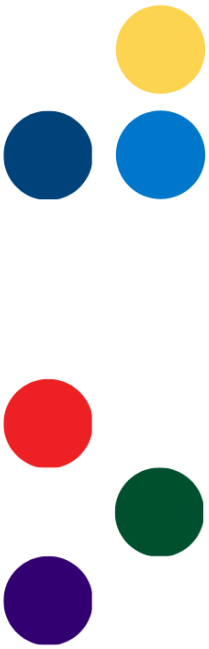
Given individual institutional ability, utilize a whole-institution approach to progressively mobilize campus partners to understand vulnerabilities and assess and mitigate risks to research spaces and sensitive research projects within existing frameworks for grant applications, such as controlled goods 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.
- More comprehensive understanding of the role of campus security and information technology teams in the delivery of research security mandates within universities.
- Canadian institutions can align and coordinate with international research security standards to avoid unnecessary risk associated with cybersecurity breaches and provide effective protection for research spaces and laboratories.

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 research information, data and equipment in sensitive research areas.



COUNCIL OF ONTARIO UNIVERSITIES

For more information, please contact:
Council of Ontario Universities
180 Dundas Street West, Suite 1800
Toronto, ON M5G 1Z8
contact@ontariosuniversities.ca

Connect with us:
www.cou.ca
www.ontariosuniversities.ca