
Government of Canada
Gouvernement du Canada
Canada
SAFEGUARDING
YOUR RESEARCH
LEARN HOW: WWW.SCIENCE.CA/SAFEGUARDING-YOUR-RESEARCH

# Canada has a strong and open research ecosystem

## Canada's science ecosystem is internationally competitive

- 1st in the OECD most-highly educated workforce[1]
  [OECD, Education at a Glance, 2017]
- Highest expenditure on higher education-performed R&D in the G7
  [OECD, MSTI 2019-1]
- 10th in the world for the quality of its research institutions
  [WEF, GCR 2018]

## World-renowned and partner of choice globally

- Strong interest of key foreign partners to deepen strategic collaborative efforts (e.g. US, UK, European Union)
- Bilateral S&T agreements with most G7 countries and several emerging economies (e.g. France, Germany, Japan, India, Israel, China, Brazil, South Korea, European Union)
- Leadership in multilateral science fora (e.g. G7, OECD, United Nations (i.e. WHO, IPCC))
- Canadians seen as honest brokers in science, development and diplomacy generating soft power.

# *That makes is an attractive target for theft or espionage by hostile individuals*

- The Government of Canada fully supports open science as essential to advancing research and innovation
- However, there is a growing awareness, domestically and internationally, of the potential for research, science, and innovation to be taken by opportunistic individuals looking to exploit research knowledge and innovation for their own benefit
- It is, therefore, important for those who fund, undertake, and support research to maintain control of their research and to decide when, how, and with whom they share their results – whether for commercial gain or public good
- Securing research is a shared responsibility of all individuals and organizations involved in research in Canada

# *These hostile individuals include those from outside the research team, or potentially members of research teams*

- **People from outside research teams or institutions** could seek to access research and researchers for their own purposes or benefits, including:
  - visiting students/faculty
  - private sector collaborators
  - foreign government representatives
  - not-for-profits
  - activists
  - commercial competitors

- **People from within research teams or institutions** could be self-motivated, supported or pressured by others to inappropriately access or steal research or innovation, including:
  - contractors
  - employees
  - students

# *The COVID-19 pandemic has demonstrated that these security risks are pressing*

- The COVID-19 pandemic has profoundly impacted Canada and the world, creating an uncertain environment for researchers under these new circumstances
  - New ways of working and communicating have created situations that malicious actors may use to advance their own interests at the expense of others

- The Canadian Centre for Cyber Security (CCCS) and CSIS recently released proactive alerts and guidance because:
  - CCCS/CSE assessed that the COVID-19 pandemic poses a heightened level of risk to the cyber security of Canadian health organizations and businesses involved in the national response to the COVID-19 pandemic
  - CSIS has also warned that Canadian intellectual property linked to the pandemic is a valuable target for state-sponsored and other actors

# *In light of this, the Government of Canada has launched a portal to provide information and guidance on how to protect your research*

- The portal was co-developed with the academic sector through the Government of Canada-Universities Working Group – a core group that engages with external stakeholders on issues regarding research security

- This *Safeguarding Your Research* portal is a public resource created to raise awareness and provide researchers with guidance and best-practices to identify and mitigate potential security risks

- The voluntary tools and guidance on the portal are meant to help all researchers – across all disciplines and organizations – safeguard their research

# *The portal highlights why safeguard research, and who you may be at risk from…*

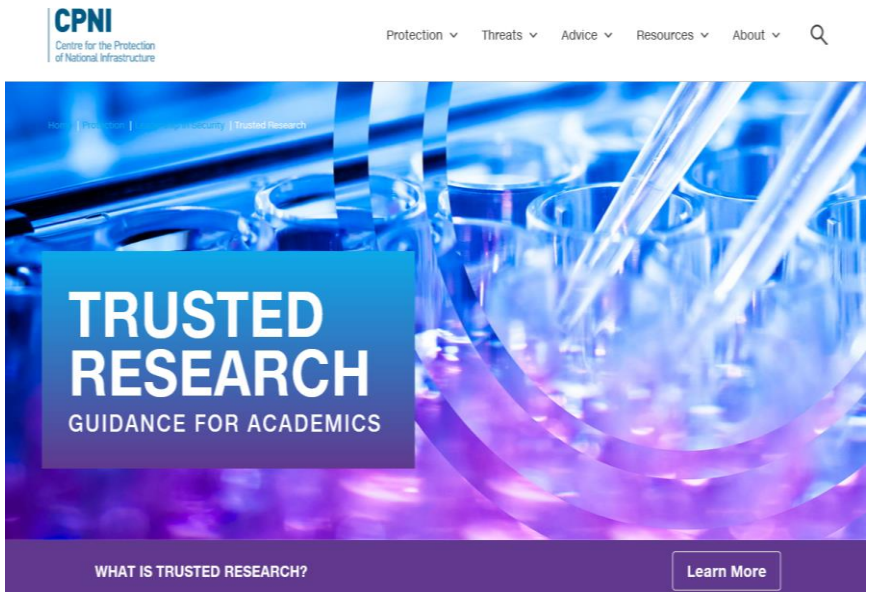
- The portal has information on why it is important to protect your research and what risks exist, including:
  - Why safeguard your research
  - Who are you at risk from
  - What are the risks
    - With case studies drawn from real world examples

- This portal will help researchers put together an effective plan on how to protect their work, with guidance on:
  - Asking the right questions
  - Helping to evaluate risk
  - Offering guidance and tools to safeguard research
  - Providing contact information for further questions

# *With links to awareness and guidance tools to help safeguard your research*

- Public Safety
  - Risk awareness
- Cyber security guidance
  - Cyber Security Advice and Guidance for Research and Development Organizations During Covid-19
  - Don’t take the bait: Recognize and avoid phishing attacks
  - Security Tips for Organizations With Remote Workers
  - Cyber Hygiene for COVID-19
  - Focused Cyber Security Advice and Guidance During COVID-19
- Knowledge and Collaboration guidance
  - Due diligence guide (to be hosted on portal)
- Travel guidance
  - CSIS Away from Home
  - Travel guidance for academics (to be hosted on portal)
- Guidance will evolve and be updated and expanded over time

# *Other guidance provided by our international allies*





- The **United Kingdom** Trusted Research program provides online guidance to post-secondary institutions and industry to raise awareness of research

- **Australia** issued Guidelines to Counter Foreign Interference, providing best practice guidance developed by a universities-government task force

- In the **United States,** the Office of Science and Technology Policy at the White House established a working group to protect federally-funded research. JASON, the independent science advisory group, produced an unclassified report assessing the degree of foreign interference in their science ecosystem and actions to improve research security

# *And includes information on what to do if research is accessed in an unauthorized way*

- Royal Canadian Mounted Police's (RCMP) National Security Information Network (NSIN) to report unrecognised people, suspicious incidents, or computer-related activities
  - RCMP NSIN Phone: 1-800-420-5805
  - RCMP NSIN Email: NSIN_RISN@rcmp-grc.gc.ca

- In the case of potential non-urgent national security threats or suspicious activities, contact the Canadian Security Intelligence Service (CSIS)
  - CSIS Phone: 1-800-267-7685
  - CSIS Website: https://www.canada.ca/en/security-intelligence-service/corporate/reporting-national-security-information.html

- For cyber security issues the CCCS Contact Centre is the single point of contact for questions on Cyber Security.
  - Phone : 1-833-CYBER-88
  - Email: contact@cyber.gc.ca

# *The Government of Canada has – in parallel – released a statement on research security*

- Co-signed by the Minister of Innovation, Science and Industry; the Minister of Health; and the Minister of Public Safety and Emergency Preparedness the statement encourages all members of the research community to be aware of the threats to their research and take precautions to protect their work

- In parallel, letters were sent to federal research funding agencies, emphasizing the shared responsibility to protect Canada's research and asking them to both work with the research community to raise awareness of these issues and to take measures to review their own security procedures and protocols