Alberta Post-Secondary Institutions Research Security Workshop
22-23 April 2024

The University of Calgary and the University of Alberta collaborated to co-host the first Alberta Post-Secondary Institutions Research Security Workshop 22-23 April 2024. The workshop focused on building capacity and connections across the province, and sharing information and best practices on priority topics with 115 registered attendees from 16 Post-Secondary Institutions, federal and provincial government and innovation accelerators.

Key Takeaways:

- Strong interest in working collaboratively to address shared challenges and priorities on research security, while recognizing each institution comes to the Community of Practice with unique contributions and requirements.
- Significant variances in resourcing, capacity, focus, structure, and priorities across Alberta necessitate a flexible approach to research security that evolves over time.
- Larger PSIs, resourced to address research security, reiterated commitments to a hub and spoke approach for collaborating and sharing knowledge, experience and resources.
- Government partners at provincial and federal levels are committed to engagement and information sharing.
- Key resourcing priorities within the community include training to build capacity; policy interpretation and guidance; risk assessment and due diligence support; cybersecurity, and coordination and administrative support.

Next Steps:

- Formalize establishment of a Community of Practice for Research Security in the province of Alberta.
- Agree on revised Terms of Reference to facilitate coordinated action and information sharing.
- Establish an Executive Committee through nomination process.
- Initiate regular meetings of the new Community of Practice to facilitate information sharing and exchange of perspectives across the varied Alberta research ecosystem.

Workshop Presentations

Government of Canada Updates

Summary:

- Representatives of the Public Safety Research Security Centre (PS RSC) and the National Science and Engineering Research Council (NSERC) provided updates on the federal government's approach to research security including forthcoming requirements relating to the Policy on Sensitive Technology Research and Affiliations of Concern.
- The primary functions of the PS RSC and the other supports available for the research community in implementing federal research security policies were elaborated.
- It was reiterated that the pertinent research security requirements will be clearly outlined for each future funding competition.
- ISED is currently consulting with Colleges, CEGEPs and Polytechnics on future research security requirements that would pertain to these institutions.

Government of Alberta (GoA) Updates

Summary:

- GoA's work on research security aligns with Goal 3 of *Alberta 2030: Building Skills for Job Strategy*,[1] and the file is led by the Ministry of Advanced Education in coordination with Public Safety and Emergency Services and the Ministry of Technology and Innovation.
- No clear updates are available at this time on whether the GoA may lift the 'China pause', but representatives did share that the Minister of Advanced Education has been briefed on a number of future options.
- The GoA understands securing research and innovation as a way to attract investments and advanced research and innovation to the province.
- The GoA is looking to Alberta PSIs for leadership and collaboration on research security through the Hub and Spoke Model. They communicated that Alberta has an opportunity to lead in creating a secure and trustworthy research and innovation ecosystem where potential partners and research innovators will want to invest.
- Considering this is a fast evolving sector, the GoA is open to dialogue with PSIs in a formal way (i.e. table, working group) to ensure that information on PSI needs and priorities, as well as decisions on research security are shared as effectively and as quickly as possible.

Research Data Management

Summary:

- Managing data across the research lifecycle involves various strategies and processes, necessitating careful planning and ongoing adaptation.

[1] Goal 3 - Support Innovation and Commercialization: Contribute to Alberta's innovation capacity by supporting post-secondary research and strengthening its commercialization potential to create new knowledge, develop future skills and diversify the economy.

- There can be tension between research security and the principles of Open Science, highlighting the need for proactive planning to identify and address gaps.
- Institutional strategies such as Data Management Plans (DMPs) and evolving RDM strategies play an important role in facilitating effective data management and stewardship.
- The introduction of pre-funding DMP templates provides targeted support for researchers to meet DMP requirements at the funding application stage, with an emphasis on ethical, legal, and commercial considerations.
- Group discussions at the workshop utilized fictional scenarios to illustrate the complexity of RDM, the importance of early addressing data-related questions, and the value of available tools to guide related conversations.

Cybersecurity

Summary:

- Cybersecurity trends and incidents experienced at U of A and U of C were outlined.
- The capacity and resources of IT departments varies widely across the province.
- Top tips and responses for cybersecurity were shared.
- Cyber threats are becoming increasingly sophisticated and leverage technologies to make attacks harder to identify or detect.
- All members of the post-secondary community must take an active role in maintaining their individual and collective cybersecurity.
- We can leverage existing tools and reach out to groups like Cybera that make their resources available to post-secondary institutions.

Artificial Intelligence and Machine Learning Presentation by Amii

Summary:

- The presenter offered an overview of the history, activities and supports of Amii as well as the Amii approach to research security. The Amii approach is to fund and lead research; use knowledge and talent to adopt AI in industry; then to inform future research through a feedback loop.
- Examples of the ways in which AI and ML can present national security risks were shared with the audience to provide a concrete look into the application of research security principles to research in these areas.
- The training that Amii offers to support AI literacy were highlighted.
- Building a culture of research security in a sensitive technology research environment (such as AI and ML) requires trust and is enhanced by personal relationships
- When research security measures break down, the entire research ecosystem is compromised which can affect others than the one project that makes the headlines (e.g. other researchers, students).

Travel and Conference Security

Summary:

- Travel, even domestic and local travel, presents risks as individuals generally travel with their entire work life on their devices while in an unfamiliar environment.
- Traveling with loaner devices containing the minimum amount of information is the safest strategy.
- Be aware of risks both digital and physical; understand your vulnerabilities and remain wary of unsolicited approaches.
- Be aware of any country-specific travel advisories provided by the Government of Canada.
- Inform the University of your travel plans early so that support can be provided via a loaner device, etc.
- Public networks are inherently unsafe, and should always be used with some kind of VPN.
- Always use your own charging cables and peripheral devices.

Research Security, Partnerships, Technology Transfer and Commercialization

Summary:

- Discussing research security issues from the earliest stages, including invention disclosure, is the best way to mitigate risks. Those responsible for technology transfer or commercialization at your institution are able to assist researchers at all stages of the process.
- Depending on the institutional IP policies and commercialization approaches, it can be difficult to advance security interests. Despite best efforts to protect research, knowledge and data these efforts can be in vain if a licensing or commercialization agreement is finalized without sufficient due diligence or consideration for national security.
- Collaboration between those responsible for technology transfer and research security can protect the interests of the individual, the institution and the country.

Open Source Intelligence

Summary:

- Combining OSINT tools enhances search comprehensiveness, requiring a clear understanding of search objectives and efficient information retrieval techniques.
- OSINT techniques should be the primary consideration rather than the specific tools. Tools are constantly changing, and the accuracy of information requires human verification.
- OSINT findings should be replicable to ensure the credibility of collected information. Considering the self-reported nature of much of this data, understanding the intended audience and objectives for sharing information is crucial.
- Privacy considerations are paramount when sharing information, particularly regarding personal data.
- Operational security is an important consideration for practitioners. It is a best practice to use a VPN while conducting OSINT investigations. The use of a virtual machine and sock-puppet accounts are also recommended. Capacity building in OSINT tools and techniques is essential, considering their complexity and evolving nature. Collaboration and information sharing among

researchers are key to optimizing tool utilization and staying updated on effective search strategies.

- SecureScholar's Beta version is nearing release. PSIs we are invited to sign up for access to Secure Scholar (pdf form) once it is ready. Unlike other OSINT tools, Secure Scholar is specifically designed to meet Canadian requirements.