Research Security Accountability and Public Acknowledgement
University of Victoria, May 2025

| Project Title | Output | Performance objectives | Performance indicators | Target outcomes |
|---|---|---|---|---|
| Research Security Contracts | $119,198 to fund a Research Security Unit staff to conduct security reviews, acquire open-source intelligence tool and implement research security considerations in research agreements and intellectual property licenses. | The objectives of this project are a) Ensure continuous delivery of OSDD and security review services to faculty and researchers in support of partnership activities such as research partnership development, funding application, research contract negotiation and technology transfer; b) Expand the implementation of OSDD to safeguard UVic research and infrastructure; and c) Subscribe access to open-source intelligence (OSINT) tool for efficient OSDD and security reviews. | • # of Risk Assessment Forms reviewed<br>• # of Due Diligence Forms completed<br>• Total value and # of funding applications supported<br>• Value and # of research agreements and intellectual property licenses processed.<br>• OSINT tool subscription renewed | Safeguard UVic research and intellectual property through the vetting of research partners and implementation of security conscious intellectual property (IP) strategy. Reduce the risk to the university with respect to the IP theft and reputational damage. Help ensure "Benefit to Canada" for research funding invested into our institution. |
| Raising Awareness for Research Security (previous titled Informing and Supporting UVIC Research and | $119,198 to fund a Research Security Unit staff to develop and deliver research security training to researchers, host workshops, and | The objectives of this project are a) Continue raising awareness of the national issue on research security within the UVic research | • # of workshops, outreach presentations and consultations | Foster a security-conscious culture and research environment at the university while respecting the core values of academic |

| | | | | |
|---|---|---|---|---|
| Creative Works for Data Confidentiality, Integrity, and Availability, and Developing Best Practices) | creating tools for open-source due diligence. | community; b) Keep faculty and researchers updated of research security-related developments of funding programs; c) Democratize OSDD to empower faculty and researchers to conduct basic vetting of partnerships; d) Proliferate best practices to UVic research community; and e) Enhance the core competency of research security personnel. | • # of faculty, researchers and research services staff trained<br>• # of briefing notes and memos released<br>• Conferences, workshops and seminars attended | freedom, transparent collaboration, open science and national security. Make the conduct of open-source due diligence seamlessly woven into the fabric of academic and research activities of UVic faculty and researchers. |
| Build Research Information Security Program (previously titled Infrastructure for Safeguarding Research program) | $164,410 on training tools, increased Research Computing Services team capacity, developing research cybersecurity training program | The objectives of this program are to a) educate UVic's research community on information security best practices; b) conduct security threat and risk assessments of research project IT solutions to identify information security risks and help mitigate those risks; c) review funding proposals and agreements, data | • Developed research information security resources.<br>• # of workshops and presentations delivered.<br>• # of security reviews/consultations conducted.<br>• # of endpoints protected by onboarding to centralized | Empower, engage and enlighten researchers to create cybersecurity culture within UVic research community. Robust information security measures applied to UVic's research environment to protect critical research data, maintain research integrity, and safeguard institutional and |

| | | | | |
|---|---|---|---|---|
| | | sharing agreements and/or any contractual agreements and help implement information security requirements as per the agreement; d) Support research information security by offering centralized institutional security solutions; e) Improved institutional tracking of research-related cybersecurity risks. | cybersecurity solution.<br>• # of vulnerability scans performed.<br>• # of faculty, researchers, and research staff engaged.<br>• # of visits to research information security website. | national interests. Hence, contributing to secure and resilient institutional infrastructure. |