

Research Security Accountability and Public Acknowledgement
University of Victoria, June 2026

Project Title	Output	Performance objectives	Performance indicators	Target outcomes
Raising Awareness for Research Security	\$100,000 to fund 1 full-time employee to deliver open-source due diligence (OSDD) training, host and coordinate research security-related workshops, provide consultation services, communicate research security updates, maintain content of the Research Security website; and participate and contribute in communities of practice.	To assist in raising awareness of research security within the UVic research and startup communities. This includes UVic faculty departments and research centers where sensitive research activities are taking place, and startups affiliated with the Innovation Centre and UVic Industry Partnerships.	- Number of workshops delivered/hosted, outreach presentations and consultations - Number of faculty, researchers, research services staff and startup personnel trained - Number of briefing notes and memos released	UVic researchers and UVic-affiliated startups are risk-aware and are exercising a risk-based approach to decision-making when pursuing partnership opportunities. By democratizing the conduct of OSDD, we empower our faculty, researchers and startups to conduct their own vetting for these opportunities, thereby molding a security-conscious culture in the UVic research and startup ecosystem that respects the core values of academic freedom, transparent collaboration, open science and national security.
Fortifying Research and Innovation Security	\$150,234 to fund 2 full-time employees that: conduct OSDD and research security reviews, assess security risks and recommend risk mitigation strategies, coordinate approval of Risk Assessment Forms, coordinate completion of research security requirements; and coordinate with security partners. We will also acquire subscription to OSINT tools.	a) Safeguard UVic research and startup ecosystem; b) Facilitate institution's compliance with Canada's NSGRP and STRAC policies; c) Facilitate institution's compliance with research security requirements of funding programs in Canada and abroad; d) Support partnerships that align with UVic's Strategic Plan, UVic's Aspiration 2030 and Canada's research security policies.	The performance indicators for this project are as follows: - Number of Risk Assessment Forms reviewed and processed - Number of Due Diligence Files completed - Total value and number of funding applications and funded partnerships vetted	UVic research and startup ecosystem is safeguarded from risks relating to unwanted transfer of dual-use intellectual properties and research results, unauthorized access to research infrastructure and foreign interference. By providing OSDD and research security review services, we support mutually beneficial partnerships wherein security risks are minimized, mitigated and managed appropriately. Ultimately, this whole initiative enables UVic researchers to access funding programs and pursue research collaboration opportunities in Canada and

				abroad, allows UVic to attract global talents and maintain its reputation as a research-intensive university, supports UVic-affiliated startups in the early stages of their high risk/high reward entrepreneurship journey, and protect Canada's national security interests.
Build Research Information Security Program (Phase II)	\$180,692	Objectives of this program are: a) educate UVic's research community on information security best practices; b) conduct security NIST 800-171 based 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 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.	• # of workshops and presentations delivered. • # of security reviews/consultations conducted. • # of faculty, researchers, and research staff engaged.	To empower, engage and enlighten researchers to create cybersecurity culture within UVic research community. To strengthen information security measures applied to UVic's research environment to protect critical research data, maintain research integrity, and safeguard institutional and national interests. Hence, contributing to secure and resilient institutional infrastructure.