Research Security Institutional Objective and Performance Table 2022-2023

Project Title	Actual Expenditures	Performance Objectives	Performance Indicators	Target Outcomes	Reported Outcomes
Research Security Centre of Excellence	$949,167	Establishing the University of Ottawa as a Research Security Centre of Excellence to enable state-of-the art security research and training.	• Completion and fit up of Cyber Hub. • Completion and fit up of Cyber Range. ○ 4 training scenarios accessible ○ 2 training tools accessible ○ 2 different tools will enable the University to be more flexible and accessible (i.e., on site and virtual) in providing training internally and to external partners, while maintain a high standard in the level of training. • Completion and fit up of Security Operation Centres. • Commence Research Security activities. • Deploy Research Security training activities. • Provide security research and experiential learning opportunities for trainees and external partners (e.g., academic institutions, government department and agencies, industry, not-for-profits, etc.).	• Enhanced opportunities for security training • Enhanced opportunities for research in security-related disciplines • Access to immersive, scenario-led exercises to upskill and reskill students and partners • Access to security-related infrastructure for research • Improved institutional position in security research for the University of Ottawa and national recognition as a centre of excellence • Access to security research and experiential learning opportunities within interdisciplinary research environments that are not currently accessible to the research community • Greater access to training programs since they will be available both on site and online	In progress. - Regarding the performance objective of establishing uOttawa as a Research Security Centre of Excellence by completing and equipping the Cyber Hub and Cyber Range, both facilities were launched in October 2023. This objective has been achieved. - Regarding the performance objective of enabling state-of -art security research and training, four training scenarios and two training tools are now accessible. However, the objective is still a work in progress. - Concerning research security activities (as a component of the Research Security Centre of Excellence), the following activities were completed: • February 2023 Creation of inaugural directorate, strategic initiatives research (security), and hiring of research security director • March and April 2023 Research Security Network developed through uOttawa and Government of Canada department. • May and June 2023 Research security stakeholder roundtable set up • August and September 2023 Senior analyst hired to support researchers • October 2023 One-stop shop launched (uOttawa webpage) to inform research community of research security matters and implement research security training activities

					• October and November 2023 Purchase of OSINT tools to support research community due diligence processes and activities - The equipping of security operation centres is still in progress. - Regarding providing security research and experiential learning opportunities for trainees and external partners (e.g., academic institutions, government department and agencies, industry, not-for-profits, etc.): • Sessions can be booked for external clients and students. • Some sessions have been delivered as part of the launch.
Research Security Tools, Process and Mechanisms	$200,950	Better position the University of Ottawa, and its research community, with tools, processes, and mechanisms to ensure excellence in research security.	• Continued maintenance and use of Contract Management system to ensure excellence research and intellectual property security. • Install and configure the core appliances of a Network Access Control Solution. • Create and define NAC policies. • Rollout NAC to pilot faculty and then to the broader research community after validation.	• Secure documentation and maintenance of contracts and intellectual property • Multiple network perimeter and endpoint security controls to prevent potential intrusion from external threats • Network Access Control (NAC) to provide automated enforcement and remediation of endpoint security threats by ensuring policy compliance for network access thus ultimately protect user and research activities.	In progress. - Regarding contract and IP management, secure software for storing contracts and IP information has been deployed. - Regarding the annual subscription for the network access control, the following actions are in progress: • Segregating the institutional network from campus • Continuous vulnerability assessment and remediation • Validation of users and assignment to them of roles to enforce access and use policies, to protect the network from security threats • Authorization, authentication and auditing of network devices (both managed and non-managed) • Role-based access control for devices, or application post-authentication • Confidentiality and containment of intellectual property through policy enforcement