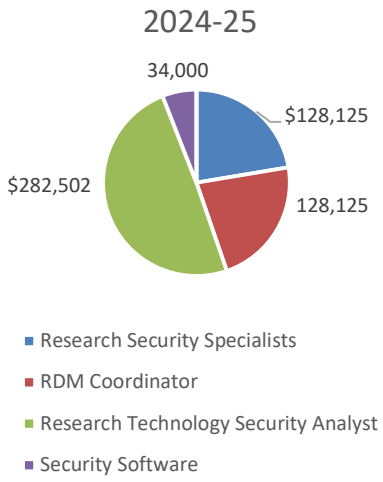
Research Security Performance Indicators



Research Security Specialists

Performance Objective

- Support researchers in their development of research security plans for their grant applications, especially around IT and cybersecurity issues, in concert with OVPR and the Library; Enable collaboration between central IT and the OVPR research security hub regarding research-related IT security and IT infrastructure; Improve university processes and supports with research ethics boards, and streamline cybersecurity vetting for researcher projects.

Performance Indicators

- Number of research security plans associated with funded research with cybersecurity considerations addressed; New frameworks and procedures around IT security and data storage for researchers to leverage; Decreased time to review for research ethics boards for data and IT-intensive research projects.

Target Outcomes

- Collaboration between central IT and the OVPR research security hub regarding

Research Data Management Specialists (RDM)

Performance Objective

- The University RDM Strategy provides a roadmap outlining how USask will support researchers at all levels in complying with funder and publisher data policies, conducting high-quality, responsible research, and applying best practices in RDM. This position will be essential in ensuring the strategy is implemented.

Performance Indicators

- Uptake on RDM training, supports, engagement from research community are all performance indicators used to monitor the success. Also, solid RDM plans in research proposals will be another indication of success. The anticipated results: The position will also result in proactive and seamless support at the application stage to ensure agency requirements are met as well as post award activities.

Target Outcomes

- Effective research data management (RDM) helps ensure research is conducted in a secure and robust manner. The RDM coordinator position will be essential in ensuring the security measures to protect research data, processes, and results are implemented in compliance with the University RDM Strategy by engaging with university senior leadership and leading campus-wide service centers in providing training and supports. The RDM coordinator will plan and implement a cohesive service model to ensure researcher-centric support for students, faculty, and staff. In addition, the coordinator will act as the main point of contact for all RDM compliance-related

Research Security Personal

Performance Objective

- Effective and proactive research security helps ensure research is conducted in a secure and robust manner. Additional positions are critical to ensuring research security and safeguarding security guidelines and requirements from funding agencies are met to reduce risk and help increase researcher success.

Performance Indicators

- Compliance, due diligence and education. The uptake on research security training and usage of tools and resources is key, along with proper compliance on applications, specifically on the risk assessment form and risk mitigation plans.

Target Outcomes

- Develop internal research security structure and tools to identify research security needs and mitigate risks. Fully leverage existing resources, establish one main point of entry, or a hub, for the research community. Minimize threats against potential risks of loss, theft or espionage, all while and maximizing success of research funding applications and projects.

Research Security Software

Performance Objective

- Purchase software that will result in quicker turnaround for researchers and the demand for research administration

Performance Indicators

- The product's ability to identify potential risk and meet the guidelines and requirements of both funding agencies and USask. Product adaptability to the changing landscape and requirements will also be a key indicator of the success.

Target Outcomes

- This tool will be central to the Research Security hub. Potential risk information will be provided to researchers and senior leaders; internal procedures will be developed to assist indecision making on how to handle information. Include fully leveraging existing resources to put in place one point of contact for the research community. hub where infrastructure by minimizing risks and maximizing success. Risk assessment forms can be completed more confidently and thoroughly, ensuring compliance with funding agency requirements and due diligence to protect USask. Contribute to the overall success in research applications and relations with funding agencies; increase sponsored research revenue, reduce financial, reputational risk and manage compliance. Minimize threats against potential risks of loss theft, unauthorized access and use. Reduce administrative burden to the USask research