University of Toronto – 2023-24 Research Security Fund – Institutional Performance Objectives

Project	Investment of Security Funds	Performance Objective	Performance Indicators	Target Outcomes	Reported Outcomes
Baycrest: Next-Gen Firewall installation	Percentage of grant invested in supporting this project: 1%	Installation of the Next-Gen firewall	To protect network using modern security standards enabling compliance with cyber security requirements and third-party service provider requirements	Increased security of network	
CAMH: Research Informatics Security Vulnerability Management	Percentage of grant invested in supporting this project: 2%	To reinforce cybersecurity through rigorous systems review and mitigation strategies using dedicated personnel	Oversight of system providing actionable information as to the specific risk, potential resolution and affected systems	Increased network security	
CAMH: Medical Imaging Database Transfer Protocol & Compliance Configuration	Percentage of grant invested in supporting this project: 2%	To implement essential security measures to support medical imaging data management for research	Providing additional security to protocol review of the medical imaging research data inclusive of MRI, CT/PET and EEG	To ensure that research data are securely transferred between source and database systems, in compliance with security requirements and complete system validation	
Holland Bloorview: Optimization of research security through enhancements and leveraging resources	Percentage of grant invested in supporting this project: 1%	To enhance on-premises research security processes by leveraging existing information security infrastructure that is employed across the hospital	To integrate the research network infrastructure into the hospital's overall technical infrastructure	Increased security by adopting cybersecurity best practices	
NYGH: Maintaining Awareness of Research Security at a Community Hospital	Percentage of grant invested in supporting this project: <1%	To better understand the risk profile and then adjust processes to reduce the risk	To discover privacy weaknesses in research networks and to educate stakeholders in best practices.	The development of standardized best practices to mitigate risk	

May 2023

HSC: Research IT Cyber security personnel and licenses	Percentage of grant invested in supporting this project: 13%	To roll out a new cyber security policy as well as ensure cyber security principles are included in data management strategies	Prepare staff to respond to security incidents, apply security patches, managing server security tools, administering the research firewall in conjunction with organization firewalls, performing network security scans	To limit security breaches and develop better procedures for response	
Sinai: Enhancing and Upgrading of Sinai Health's research cyber security	Percentage of grant invested in supporting this project: 5%	Renewal of LTRI antiviral programs	Installation of Veeam backup management; Nakivo backup management system; Disaster Recovery offsite software	Implementation of all project elements in expected timeframe	
Sunnybrook: Cybersecurity infrastructure updates for SRI and threat detection and preventative maintenance	Percentage of grant invested in supporting this project: 6%	Installation of Crowdstrike on Linux and specialized equipment machines	Proactively assessing vulnerabilities of potential cyber threats on critical research systems as well as REDCap environment	Implementation of all project elements in expected timeframe	
Trillium: Corporate Research Risk and Privacy Management and Quality Assurance	Percentage of grant invested in supporting this project: <1%	To ensure all contracts and agreements meet with all security and privacy requirements	To address research related operational issues and risks presented by the organizations research engagement activities	Increased network security	
Trillium: Institutional Research Data Management (RDM) Strategy	Percentage of grant invested in supporting this project: <1%	To create systems and processes for researchers providing guidelines to ensure best practices	To develop RDM strategies and Data management plans to identify security gaps in institutional data sources	To limit security breaches and develop better procedures for response	
Trillium: RCR/Integrity Framework and Practice Change	Percentage of grant invested in supporting this project: <1%	To reframe and revitalize research integrity/RCR through education and culture	To plan engagement sessions to identify privacy gaps and target areas of high risk	Increased network security	
Trillium: Research Partnership Security	Percentage of grant invested in supporting this project: <1%	To mitigate security risks in research when engaging with international research partnerships	To assist in the development of practices/processes/guidelines around mitigating risk with international research partnerships	Greater stakeholder engagement in the development of principles and best practices in international collaborations.	

Trillium: Review, assess and prioritize etools to optimize operations	Percentage of grant invested in supporting this project: <1%	To build a new electronic tool that will serve as a real-time enterprise management system	Increased security across research operations and innovation projects	To complete project within anticipated timelines	
Trillium: THP Data Platform Development	Percentage of grant invested in supporting this project: <1%	To manage security risk for the AWS Platform	To maintain the security of AWS cloud environment	To complete project within anticipated timelines	
Trillium: Update and revalidation of all Legal, Liability, Privacy and Security Templates and Standard Provision documents	Percentage of grant invested in supporting this project: <1%	To review and update all agreement and contract templates to meet new legal, risk and privacy requirements	To review and update all our legal and liability tools, standard provisions, advice repository and supporting documents to ensure that they align with changing business, regulatory, operational and security and privacy requirements	To complete project within anticipated timelines	
UHN: Implementing Beyond Trust Solution	Percentage of grant invested in supporting this project: 3%	Implementing Beyond Trust Solution within the UHN Environment as the Privileged Access Management (PAM) solution, restricting access to critical back-end servers	To allow better control and access by privileged account users to our environment which runs the Research enterprise	To complete project within anticipated timelines	
UHN: Implementing CrowdStrike as the EndPoint Security Solution	Percentage of grant invested in supporting this project: 3%	Configuring CrowdStrike solution on all Research managed Endpoints and servers	To provide 100% coverage of Research End User Devices and server protection	To complete project within anticipated timelines	
UHN: Implementing Vulnerability Management Solutions	Percentage of grant invested in supporting this project: 2%	To implement Bitsight, Netsparker, Tenalbe and Armis	To provide 100% coverage of the research environment	To complete project within anticipated timelines	
UHN: Implementing Security Monitoring Solutions	Percentage of grant invested in supporting this project: 2%	To implement SPLUNK Solution	To provide 100% coverage of the research environment	To complete project within anticipated timelines	

UHN: Implementing “Proof-Point” as the Email Security and awareness Solution	Percentage of grant invested in supporting this project: 3%	To configure ProofPoint solution for all research active mailboxes	This tool will protect users from dangerous emails/attachments by stopping them before they reach user inboxes	To complete project within anticipated timelines	
UHN: Implementing Network Security Solutions	Percentage of grant invested in supporting this project: 2%	To implement Forescout and Gigamon	To provide 100% coverage of the research environment	To complete project within anticipated timelines	
Unity Health: Reinforcing Research Data, Informatics and Operational Integrity	Percentage of grant invested in supporting this project: 8%	To develop a model to create a reinforced, redundant and recoverable digital environment	Improvements will increase transparency, accountability and compliance to the ever evolving global and regional jurisdictional requirements that govern research data and intellectual property	The final deliverable will be full accounting of existing research assets, their associated vulnerabilities, possibilities for enhancements, and a roadmap to an integrated state-of-the-art digital infrastructure that meets the latest industry standards	
WCH: Investigating security gaps to prevent data breach or exploitation within REDCap environments	Percentage of grant invested in supporting this project: 1%	To allow for a dedicated part-time Applications Specialist to provide support for existing security processes as well as investigate security gaps to minimize risks	To test vulnerabilities, document strategies to mitigate security issues	To complete project within anticipated timelines	
UT: Research Security Staffing	Percentage of grant invested in supporting this project: 15%	To hire four Research Security Advisors to assess and augment the needs of the University’s three campuses, 17 academic divisions, 4,000+ faculty, 100,000 students, 9,000 active research funds and hundreds of international research partnerships	To pro-actively support the research, analysis, preparation, submission, review, and ongoing administration of research security plans /strategies and carry out related activities.	Hiring of Advisors	

University of Toronto – 2023-24 Research Security Fund – Institutional Performance Objectives

UT: Research Security Software	Percentage of grant invested in supporting this project: 8%	To invest in new software to support developing research security program. These tools provide information regarding connectivity to entities of concern and the potential for human rights abuses	To aid with research security on all research in sensitive sciences, grants, partnerships, and memoranda of understanding,	To implement software in desired timelines	
UT: Secure Loaner Devices for International Travel	Percentage of grant invested in supporting this project: 4%	To provide traveling personnel with loaner secure laptops and mobile phones in order to mitigate the risk of disclosure of sensitive and/or proprietary information	To develop and maintain hardware and software configurations (e.g., patching, upgrading, applying security best practices, complying with research export restrictions, etc.)	To have devices maintained and secure in desired timelines	
UT: Research Information Security Analysts	Percentage of grant invested in supporting this project: 9%	Contracting three cybersecurity analysts in the Information Security Team to align departmental practices to institutional approaches to reduce risk to Canadian research by implementing protection, detection, and response cyber security controls	Aid in identifying and mitigating research security risks	Outcomes include: 1) reviewing and updating risk management plans; 2) classifying data assets; 3) detecting and remediating critical computer vulnerabilities; and 4) implementing next-generation end-point protection software	
UT: Research Intensive Group	Percentage of grant invested in supporting this project: 2%	To enhance the collective security postures of institutions across Canada	To develop proof of concepts related to Advanced Detection and Response and Dark Web Monitoring	Identify and mitigate risks to research security	

May 2023

UT: Physical Research Security	Percentage of grant invested in supporting this project: 6%	To promote added safety for research facilities of all kinds, a number of buildings are being upgraded to a higher level of access control as recommended by the Tri-Campus Physical Security Working Group	Implementation will ensure a very low number of incidents of unauthorized access and/or thefts from / damage to research facilities, and a reciprocal increase is the sense of security of those who work in or around those facilities	To provide high level access control to over 60 buildings in the life cycle of the project.	
UT: A Secure Data Repository using UofT Dataverse in Borealis: Expanding Support for Researchers with Access- Limited Data	Percentage of grant invested in supporting this project: 2%	To (1) assess the U of T Dataverse for any gaps that must be addressed to offer secure handling of level 3 and 4 research data, (2) recommend the best methods of addressing these gaps (3) produce a report detailing these findings	Assist in coordinating research security across the Dataverse in Borealis	Identify and mitigate risks to the Dataverse in the Borealis	