University of Toronto – 2024-25 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	Completed installation of Endpoint Detection and Response (EDR) on all computers, achieving 100% device coverage and meeting cybersecurity insurance requirements to strengthen network protection and reduce organizational risk exposure.
Baycrest: Cybersecurity EDR implementation phase 2	Percentage of grant invested in supporting this project: <1%	The installation of Antivirus/Antimalware software	An increase in the breadth of coverage required to further reduce the potential attack surface	Compliance with our IT policy, and cyber-insurance and third party service provider requirements will be realized	Installed Next-Generation Firewall across the network, meeting cybersecurity requirements and enhancing protection against advanced threats, ensuring compliance with security standards and reducing organizational risk exposure.
CAMH: Research Informatics Security Vulnerability Management	Percentage of grant invested in supporting this project: 1%	The objective of CAMH's Research Informatics Security Vulnerability Management project is to reinforce CAMH's cybersecurity through rigorous systems review and mitigation strategies using dedicated personnel	Vulnerabilities are tracked using commercial software and monitoring tools into critical, important, moderate and low categorizations.	Increased network security	Cybersecurity risks across CAMH's research infrastructure were systematically identified, prioritized, and resolved. Continuous monitoring, timely patching, and vulnerability management ensured robust oversight, actionable insights, and compliance, significantly reducing high, medium, and low-risk exposures.
CAMH: Harmonized MFA (DUO) & Research Storage Ransomware Protection	Percentage of grant invested in supporting this project: 3%	Upgrades to Harmonized Multi-Factor Authentication (DUO) and Research Storage Ransomware Protection	Increase the percentage of CAMH applications protected by DUO from its current level to 100% by the target date, and reduce unauthorized access incidents by 50% within six months after implementation	To complete project milestones in timely manner	Implemented DUO multi-factor authentication across critical applications and deployed ransomware protection for research storage systems, achieving high user adoption, enhanced security, rapid recovery capability, and uninterrupted operational continuity for CAMH's research infrastructure.

October 2025

University of Toronto – 2024-25 Research Security Fund – Institutional Performance Objectives

Project	Investment of Security Funds	Performance Objective	Performance Indicators	Target Outcomes	Reported Outcomes
Holland Bloorview: Enhancing cybersecurity of research network	Percentage of grant invested in supporting this project: 1%	Undergo cyber security assessments of our research network and implement any measures identified by the assessment	The identification of risks to the network	Mitigate those risks	Completed cybersecurity assessments of cloud and MRI PACS applications and implemented recommended measures, strengthening configurations, mitigating vulnerabilities, and ensuring compliance with best practices to enhance Holland Bloorview's research network security and resilience.
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 and to stay aligned with the continuously evolving federal guidelines and tools for protecting research	Raised research security awareness through updated intranet guidelines, orientations, and improved access processes; funded coordinator role to implement safeguards, ensuring compliance and reducing risks for researchers at North York General Hospital.
HSC: Comprehensive Cybersecurity Initiative	Percentage of grant invested in supporting this project: 13%	To enhance the security posture of the research enterprise through the implementation of advanced security solutions	The Enterprise Cyber Security Endpoint Protection and Privileged Access Management initiative aims to implement Privileged Access Management and Microsoft Defender for Endpoint solutions to protect the confidentiality, integrity, and availability of research data and systems.	Safeguarding sensitive data and Research Institute infrastructure against potential cyber threats	Implemented privileged access management and endpoint protection across Research IT and HPC infrastructure, achieving full compliance, enhanced threat detection, operational efficiency, and secure collaboration while validating HPC4Health's PHI safeguards through independent assessment and remediation.

October 2025

University of Toronto – 2024-25 Research Security Fund – Institutional Performance Objectives

Project	Investment of Security Funds	Performance Objective	Performance Indicators	Target Outcomes	Reported Outcomes
Sinai: Enhancing and Upgrading of Sinai Health's research cyber security	Percentage of grant invested in supporting this project: 4%	The enhancement, continuation and upgrading of crucial elements to Lunenfeld-Tanenbaum Research Institute's cyber security platforms	Renewal of various software and hardware platforms	Implementation of all project elements in expected timeframe	Enhanced research cybersecurity by replacing legacy VPN and firewall with modern integrated platforms, enforcing MFA, improving endpoint visibility, and enabling real-time threat detection, reducing operational risk and strengthening compliance across remote and on-prem environments.
Sunnybrook: IT Block Storage System Project - Security Infrastructure	Percentage of grant invested in supporting this project: 7%	To complete a critical upgrade to local and centralized data storage facilities to comply with Tri-Council data management requirements and to address business continuity and expedient data restoration requirements	New agreements for data storage solutions that is centrally managed and secured for PHI and secure corporate data storage, including robust backup functionalities and data restoration software	Implementation of all project elements in expected timeframe	Implemented a new block storage array with optimized storage pools, reducing critical data restoration time from six months to 72 hours, significantly improving research data resilience and operational continuity.
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 security and privacy requirements	To address research related operational issues and risks	Increased security and compliance	Ensured all research contracts met security and privacy requirements, reducing escalations by 25% and QA review time by 50%, while improving staff efficiency through standardized checks and team-based learning.
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	Established secure systems, centralized storage, and RDM policies aligned with FAIR principles; delivered researcher training to ensure compliant data access, use, and sharing, protecting sensitive information and supporting Tri-Agency requirements.

October 2025

University of Toronto – 2024-25 Research Security Fund – Institutional Performance Objectives

Project	Investment of Security Funds	Performance Objective	Performance Indicators	Target Outcomes	Reported Outcomes
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	Reduced risk and compliance issues	Conducted gap analysis and engagement surveys to identify needs; initiated co-designed educational outputs and planned focus groups to strengthen research integrity culture through continuous validation and uptake assessment.
Trillium: Formation of a novel Artificial Intelligence (AI) Research Ethics Board (REB)	Percentage of grant invested in supporting this project: <1%	To create an REB focused on AI research that can maintain pace with technological changes	Creation of new AI research document	Implementation of all project elements in expected timeframe	Established AI-focused REB with diverse membership, developed reviewer criteria and guidance documents, obtained expert feedback, initiated training, and created a financial sustainability model to address emerging ethical concerns in AI research.
Trillium: Review, assess and prioritize etools to optimize operations	Percentage of grant invested in supporting this project: <1%	To construct an 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	Developed Version 1 of a real-time research administration platform through user-centered design and testing, automating core processes with security controls; secured vendor for assessments and confirmed phased release schedule.
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	Initiated comprehensive update of legal and privacy templates, refined standard provisions to include research security, open science, RDM, and AI considerations; secured external counsel and aligned scope, timeline, and risk thresholds.

October 2025

University of Toronto – 2024-25 Research Security Fund – Institutional Performance Objectives

Project	Investment of Security Funds	Performance Objective	Performance Indicators	Target Outcomes	Reported Outcomes
UHN: AD Consolidation of UHNRESEARCH servers and mailboxes	Percentage of grant invested in supporting this project: 1%	Consolidate UHNRESEARCH.CA with UHN.CA domain for more seamless user network access and consistent workflows and manage identities more centrally from a security standpoint	Unified and managed IDM customer experience	To complete project within anticipated timelines	Consolidated UHNRESEARCH.CA into UHN.CA, achieving unified login, centralized identity management, MFA enforcement, and improved security across platforms; major milestones completed, with remaining storage permissions and cleanup tasks in progress toward full decommissioning.
UHN: Implementing Data Security Solutions within the UHN Environment	Percentage of grant invested in supporting this project: 3%	To implement various tools and platforms to prevent against dark web threats	To provide 100% coverage of Research End User Devices and server protection again dark web threats	To complete project within anticipated timelines	Deployed Cybersixgill and Horizon3AI to enhance threat intelligence and vulnerability management, achieving near 100% alert coverage; improved dark web monitoring and automated remediation, with Varonis implementation planned to strengthen data governance.
UHN: Incorporation of Michener into UHN Cyber Tools	Percentage of grant invested in supporting this project: 3%	Implementing CrowdStrike endpoint detection, Tenable, Gigamon and BeyondTrust	Complete onboarding onto all applicable UHN security tools	To complete project within anticipated timelines	Onboarded Michener to UHN cybersecurity tools, deploying CrowdStrike EDR and Spotlight for advanced threat detection and vulnerability management; improved security posture and alignment with enterprise standards, with Gigamon traffic visibility deployment delayed to October 2025.
UHN: Research Firewall Migration and Rule Clean Up within Palo Alto	Percentage of grant invested in supporting this project: 4%	The scope of this project is to enhance the existing UHN network firewall technology by migrating legacy research firewalls on pfSEnse to Palo Alto 5450 firewalls	Migration of all legacy research firewalls and rulesets to Palo Alto 5450 firewalls	To complete project within anticipated timelines	Migrated all legacy pfSense firewalls to Palo Alto 5450, improving performance and security; centralized management achieved, with firewall rule cleanup in progress to eliminate outdated configurations and align with cybersecurity standards.

October 2025

University of Toronto – 2024-25 Research Security Fund – Institutional Performance Objectives

Project	Investment of Security Funds	Performance Objective	Performance Indicators	Target Outcomes	Reported Outcomes
UHN: Implementing TINES Solutions for automating security incident response workflows within UHN	Percentage of grant invested in supporting this project: 1%	Implementation of "TINES" solution	Configure automated security incident response workflows for a reduction in the number of false positive threats	To complete project within anticipated timelines	Implemented TINES automation for security incident response, reducing false positives and MTTR through enriched alerts, phishing triage, and real-time containment actions, improving efficiency, governance, and alignment with cybersecurity standards across UHN Research.
UHN: Implementing Network Security Solutions	Percentage of grant invested in supporting this project: 1%	Configuring an updated Network Security solution for Research cyber monitoring during	To provide 100% coverage of the research environment	To complete project within anticipated timelines	Upgraded Gigamon appliances to achieve 100% network traffic visibility, including east-west monitoring, improving threat detection, operational efficiency, and compliance; integrated seamlessly with existing security tools without disrupting research operations.
UHN: Clean Up of Internet Exposed Websites in Research	Percentage of grant invested in supporting this project: 3%	Web inventory to ensure full compliance to information security standards	0 internet exposed websites	To complete project within anticipated timelines	Upgraded Gigamon appliances to achieve 100% network traffic visibility, including east-west monitoring, improving threat detection, operational efficiency, and compliance; integrated seamlessly with existing security tools without disrupting research operations.
Unity Health: Evaluating Security of Research Information Systems	Percentage of grant invested in supporting this project: 8.2%	To identify security gaps in research information systems and provide remediation	To conduct a penetration test and to revise policies/procedures documents, and implement recommended security controls.	To complete project within anticipated timelines	Completed vulnerability assessment and penetration test with actionable reports; remediated all critical and high-severity findings, revised policies, and strengthened REDCap Academic's security posture to protect sensitive research data and ensure compliance.

October 2025

University of Toronto – 2024-25 Research Security Fund – Institutional Performance Objectives

Project	Investment of Security Funds	Performance Objective	Performance Indicators	Target Outcomes	Reported Outcomes
WCH: Investigating security gaps to prevent data breach or exploitation within REDCap environments	Percentage of grant invested in supporting this project: 1%	This year will further focus on development of a formal plan for REDCap testing as well as guidance documents on validation of Health Canada regulated environments (e.g. lessons learned and best practices).	To test vulnerabilities, document strategies to mitigate security issues	To complete project within anticipated timelines	Developed comprehensive REDCap testing plan with regulatory alignment, initiated guidance documents for Health Canada environments, drafted SOPs, validated external modules, and advanced automation strategies to strengthen compliance, security, and operational efficiency.
UT: Research Security Staffing	Percentage of grant invested in supporting this project: 22%	We have hired 4 Research Security Advisors, and will be adding a Research Security Data Analyst, to serve 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 increase awareness and adherence to research security protocols, mitigating risks, addressing threats and enabling world-class research to move forward	Success of the investment will be assessed through monitoring the range and value of services provided and 'customer satisfaction', but ultimately determined by the absence of instances where research is delayed or interrupted by research security issues.	Established advisory and analyst roles to provide confidential geopolitical risk guidance, interpret evolving security requirements, support research security plans, and develop data intelligence tools, strengthening compliance and safeguarding research collaborations.
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	Implemented advanced Data-as-a-Service platforms to scale research security analysis, enabling strategic insights and compliance with Tri-Agency requirements across UofT's large research portfolio through automated, high-volume data assessments.

October 2025

University of Toronto – 2024-25 Research Security Fund – Institutional Performance Objectives

Project	Investment of Security Funds	Performance Objective	Performance Indicators	Target Outcomes	Reported Outcomes
UT: Secure Loaner Devices for International Travel	Percentage of grant invested in supporting this project: 1%	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	Established secure travel device program with 20 laptops and 10 burner phones for academics visiting high-risk regions; implemented baseline hardening, forensic analysis on return, and delivered joint security guidance sessions.
UT: Research Information Security Analysts	Percentage of grant invested in supporting this project: 8%	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	Expanded Cybersecurity-as-a-Service to nine faculties, embedding experts to accelerate security adoption; remediated 132 vulnerabilities, improved risk management, reduced incident response time by 92%, deployed endpoint protection, and delivered training to strengthen research security posture.
UT: Research Intensive Group	Percentage of grant invested in supporting this project: <1%	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	Piloted Federated SOC across nine institutions, detecting 1,800+ monthly threat alerts previously unseen; deployed Honeypot service at 14 institutions to identify malicious activity early and strengthen sector-wide cyber defenses.
UT: Physical Research Security	Percentage of grant invested in supporting this project: 2%	To promote added safety for research facilities; upgrade buildings 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.	Enhanced emergency response capabilities with rapid research building lockdown, reducing critical incident response times and increasing staff and student confidence in workplace security and protection of sensitive research assets.

October 2025

University of Toronto – 2024-25 Research Security Fund – Institutional Performance Objectives

Project	Investment of Security Funds	Performance Objective	Performance Indicators	Target Outcomes	Reported Outcomes
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: 4%	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	Strengthened Borealis repository security through infrastructure-as-code, CI/CD automation, encryption, and access controls; completed gap analysis, published sensitive data guidelines, advanced national partnerships, and initiated remote storage pilots to support scalable, compliant research data management.

October 2025