University of Toronto – 2025-26 Research Security Fund – Institutional Performance Objectives

Project	Investment of Security Funds	Performance Objective	Performance Indicators	Target Outcomes	Reported Outcomes
Baycrest: Network Firewall Feature and Security Expansion	$20,633	Enhance institutional cybersecurity by upgrading the firewall to actively scan and automatically block advanced threats.	Automated threat interception statistics and Ongoing absence of security breaches as verified by secondary defenses.	Enhanced network security, sustained protection against unauthorized access, and increased resilience to cyber threats.	
CAMH: Secure AI & Data Governance Infrastructure for Research MLOps	$135,000	Develop a secure, governed AI infrastructure within CAMH's research environment to enhance cybersecurity, reproducibility, and compliance with national research security standards.	Metrics include the number of secure model pipelines deployed, users onboarded, percentage of models with auditable histories, logged security incidents, and completion of SOPs and infrastructure hardening.	A fully operational, secure MLOps ecosystem with traceable, reproducible AI workflows, aligned with CAMH's governance framework and national security priorities.	
CAMH: Data Security for Sensitive Clinical and Genomic Research Repositories	$42,426	Enhance the security of CAMH's sensitive research data environments (HDN and BHDB) by implementing advanced encryption, secure data transfer, and real-time threat monitoring systems.	Key metrics include the percentage of repositories with encryption-at-rest, number of threats detected and resolved, secure data transfers via Globus, backup integrity tests, and completion of quarterly audits.	A robust, monitored infrastructure that protects sensitive health and genomic data, ensures regulatory compliance, and sets a national standard for secure research data stewardship.	
Holland Bloorview: Enhancements to Research Digital Platforms	$35,042	Ensure all data platforms used in regulated clinical trials at Holland Bloorview meet compliance, validation, audit, and cybersecurity requirements.	Number of platforms, software, and digital tools that comply with regulatory standards.	Robust data documentation and management that upholds data integrity, supports scientific advancement, and ensures compliance with clinical trial regulations.	
NYGH: Maintaining Awareness of Research Security at a Community Hospital	$3,144	Enhance research security awareness and risk mitigation at North York General Hospital by monitoring evolving threats, updating internal guidelines, and refining access and ethics review processes.	Number of exceptions to standard access protocols and researcher feedback on security awareness initiatives.	A more secure and informed research environment with improved adherence to national research security standards.	

HSC: Plan of Action and Milestones (POAM) for Cyber Security Remediations	$539,018	Develop and implement a multi-year Plan of Action and Milestones (POAM) to address cybersecurity and privacy risks identified in third-party assessments and align with NIH security best practices.	Progress on POAM implementation, completion of business continuity planning, remediation of identified cyber deficiencies, and system alignment with NIH and NIST standards.	A strengthened security posture for SickKids' research infrastructure, enabling secure access to high-value datasets, ensuring compliance, and supporting continued national and international research collaborations.	
Sinai: Enhancing and Upgrading Sinai Health's Research Cyber Security Stance.	$182,160	Enhance and maintain the cybersecurity infrastructure at Lunenfeld-Tanenbaum Research Institute by renewing critical software and hardware components to reduce vulnerabilities and improve disaster recovery capabilities.	Deployment and renewal of key cybersecurity tools (e.g., Microsoft Defender Plan 2, Intune, Nessus, VPN, antivirus, backup systems), and completion of third-party application architecture reviews.	A more robust, secure, and resilient IT environment that minimizes the attack surface and ensures continuity and protection of research systems and data.	
Sunnybrook: Research Staff Recruitment, Retention and Training	$142,939	Strengthen research security at Sunnybrook Research Institute by recruiting skilled cybersecurity staff and implementing comprehensive, role-specific training programs.	Metrics include recruitment of staff with security designations, 90% participation in annual refresher training, positive feedback on interactive scenarios, and training coverage for high-risk research areas.	A well-trained, security-aware research workforce that aligns with national security priorities and protects critical institutional assets by 2027.	
Sunnybrook: Secure Research Network and Cloud Computing Services	$85,134	Establish a secure, compliant, and scalable research network to protect high-sensitivity data and support innovation at the research institute.	Metrics include 100% migration of high-risk projects to the Secure Research Network (SRN), 24/7 monitoring with monthly audit reports, and successful third-party	A fully operational, monitored, and certified SRN by April 2028 that meets national cybersecurity standards and enables secure, cutting-edge research.	
Trillium: Formation of a novel Artificial Intelligence (AI) Research Ethics Board (REB)	$487	Establish a dedicated AI Research Ethics Board (REB) to ensure ethical, fair, and secure oversight of AI research, addressing emerging concerns like bias and health inequity.	Recruitment of diverse REB members, development of AI-specific ethics documents and SOPs, and completion of training and CTO qualification review.	A fully operational AI REB that provides expert guidance, supports responsible AI research, and ensures alignment with evolving ethical and regulatory standards.	
Trillium: Develop Research Data Repository	$600	Develop a centralized, secure, and regulation-compliant research data repository through a co-design process with institutional stakeholders.	Engagement of researchers for input, collaboration with internal and external partners to select a platform, and creation of a repository framework with community feedback.	A functional, centralized data repository that supports secure data storage, regulatory compliance, and long-term data retention aligned with Tri-Agency RDM policy.	

Trillium: Implementation of New Agreement Templates and Standard Provision Document	$468	Support the effective implementation of new research templates and the Standard Provision Document (SPD) by identifying and addressing user training and support needs.	Established implementation plan, defined performance metrics, and assessment of training, orientation, and advisory requirements.	Successful adoption and impact measurement of the new tools through tailored support and structured implementation.	
Trillium: SOURCE Survey Implementation and Project Oversight	$1,229	Evaluate changes in the research integrity climate at THP by conducting a second SOURCE survey in collaboration with NCPRE.	Completion and analysis of the survey, and development of a report and action plan based on the findings.	Data-driven insights to inform future initiatives that strengthen research integrity across the organization.	
Trillium: Optimize and Scale Research Security Process, Practice & Infrastructure in support of 3 - 5 year Research Plan	$1,877	Optimize and scale research security processes, practices, and infrastructure to align with corporate research priorities over the next 3–5 years.	Completion of risk and impact assessments, implementation of evidence-based optimization strategies, and post-implementation reassessment of research security systems.	A more robust, efficient, and aligned research security framework that supports long-term institutional research goals.	
Trillium: Integration and Adoption of Research Security Process, Practice & Infrastructure in Corporate Clinical Trials Strategy	$4,549	Integrate research security processes, practices, and infrastructure into the corporate clinical trials strategy to support secure and compliant trial operations.	Identification and evaluation of research security requirements, incorporation of best practices into the Clinical Trials Strategy Roadmap, and development of an integration and adoption plan.	A secure, scalable clinical trials framework that aligns with emerging research security standards and supports the organization's strategic goals.	
Trillium: Enhance Capabilities related to Research Security for AI Research and Data Management through AI & Data Research Ethics Lead Role Pilot	$1,395	Pilot an AI & Data Research Ethics Lead role to enhance research security capabilities for AI research and data management at the corporate level.	Evaluation and integration of research security requirements into governance documents, and development of educational resources and sessions for the research community.	Improved institutional readiness and governance for secure, ethical AI research and data management through dedicated leadership and community engagement.	
Trillium: Integration of Research Security Process, Practice & Infrastructure in New Enterprise Technology Solution and Change Management Strategy	$2,891	Integrate research security processes, practices, and infrastructure into the new THP research enterprise technology solution and its change management strategy.	Incorporation of best practices into the system's technical architecture and implementation of a structured integration and adoption plan.	A secure, future-ready research technology platform that embeds research security into both system design and organizational processes.	

Trillium: Integration of Research Security Process, Practice & Infrastructure in Intellectual Property Policy Assessment & Implementation Plan	$768	Develop and implement an evidence-informed intellectual property (IP) policy that integrates research security considerations throughout the IP lifecycle.	Completion of an updated environmental scan, integration of best practices into the new IP policy, and development of a corresponding implementation plan.	A secure, compliant IP management framework that aligns with emerging research security standards and supports responsible innovation.	
UHN: Implementation of Netwrix Secure Password Strengthening Tool	$21,826	Implement the Netwrix Password Strengthening Tool to enforce stronger password policies and reduce the risk of unauthorized access by July 2025.	Percentage of users meeting new password standards, number of password-related service desk tickets, and average password resets per user.	Improved password security, reduced IT support demands, enhanced user experience, and better compliance with institutional security policies.	
UHN: Enhancing Web Security with Cloudflare	$76,603	Deploy Cloudflare's Web Application Firewall (WAF) to protect UHN web applications from common exploits and reduce brute force login attempts by January 2026.	Metrics include the number of blocked threats per month, reduction in successful brute force login attempts, and the percentage of traffic routed through Cloudflare.	Enhanced web application security, reduced system overload, and improved access control that minimizes disruptions for legitimate users while blocking malicious traffic.	
UHN: Cloud Security: Zero Trust Network Access (ZTNA) for Unmanaged Devices	$132,366	Enroll all unmanaged devices into a Zero Trust Network Access (ZTNA) framework by April 2026 to eliminate direct network access and enforce role-based access controls.	Percentage of unmanaged devices onboarded (target: 100%) and successful implementation of access policies restricting users to only authorized applications and resources.	Reduced risk of data breaches, improved control over remote access, and enhanced data protection through strict access policies and data loss prevention measures.	
UHN: UHN Digital Security Program - Implementing Crowdstrike Identity and Exposure Management Modules in the UHN Environment	$130,663	Deploy CrowdStrike Identity Protection and Spotlight across all domain controllers and servers to detect identity-based threats in real time and reduce critical vulnerabilities by March 2026.	100% deployment coverage, reduction in stale accounts, average time to resolve identity-related incidents, and number of servers tagged and scanned for vulnerabilities.	Improved threat detection, faster incident response, reduced identity-related risks, and enhanced visibility and remediation of system vulnerabilities across UHN's research and enterprise environments.	
UHN: Implementation of Data Loss Prevention Tool (Varonis)	$100,899	Implement the Varonis Data Loss Prevention (DLP) tool to automatically classify sensitive data and enable real-time alerts for improper data sharing by April 2027	Percentage of data classified, reduction in improper sharing of sensitive data, and decrease in data sharing violations.	Enhanced data visibility and control, reduced risk of data breaches, improved compliance readiness, and a stronger overall security posture.	

UHN: Bitsight Score Improvement: Remediation of Internet Exposed Websites	$75,427	Create a complete, categorized inventory of all internet-exposed websites under the organization's jurisdiction and ensure 100% compliance with updated security standards by September 2025.	Percentage of websites inventoried and classified by data sensitivity, percentage meeting security standards, and number of non-compliant sites taken offline and remediated.	A secure, policy-compliant web presence that reduces breach risks, protects sensitive data, and supports long-term governance and operational efficiency.	
UHN: Establishing Research Partnership Security & Compliance Capacity at UHN	$113,423	Establish an institutional framework at UHN to assess and mitigate research partnership security risks by streamlining review processes and	Development and implementation of a review algorithm and SOP, and tracking of review timelines and mitigation plan implementation.	A more efficient, transparent, and consistent approach to managing research partnership risks, enhancing institutional capacity and compliance with evolving security requirements.	
Unity: Enhancing EDC Security/Resilience Through Migration from MySQL Community to MariaDB Community	$284,474	Upgrade UHT's Redcap Academic database from MySQL to MariaDB Community Edition to enhance security, compliance, and operational resilience in managing sensitive healthcare research data.	Successful migration with zero data loss, implementation and verification of at-rest encryption, improved backup/restore performance, reduced downtime, and compliance with PHIPA and institutional security standards.	A more secure, efficient, and compliant Redcap system with improved data protection, reduced operational risk, and long-term compatibility with Redcap's lead development institution.	
WCH: Investigating security gaps to prevent data breach or exploitation within REDCap environments at Women's College Hospital	$52,660	Enhance the security and regulatory compliance of Women's College Hospital's REDCap platform by strengthening system configurations, conducting regular security testing, and developing robust documentation and procedures.	Successful completion of quarterly security audits (e.g., penetration testing, SQL injection, XSS), implementation of SOPs, log and plugin reviews, and validation of encryption and access controls.	A more secure, resilient REDCap environment that protects sensitive research data, meets regulatory standards, and supports ongoing research involving high-risk and marginalized populations.	
UofT: Research Security Staffing in VPRI	$1,149,001	Sustain and expand the University of Toronto's Research Security Team (RST) to support compliance with national and international research security policies, while enabling secure, world-class research across its campuses and partnerships.	Range and value of services provided, researcher and stakeholder satisfaction, and the success rate of applications meeting research security requirements.	A robust institutional framework that proactively manages research security risks, supports compliance with evolving policies, and strengthens U of T's leadership in secure, globally collaborative research.	

UofT: Research Security Software	$336,574	Leverage advanced data analytics platforms (Strider and Kharon) to enhance research security assessments and ensure compliance with federal policies such as NSGRP and STRAC.	Number of collaborators and partners analyzed using these tools, and alignment of internal assessments with Government of Canada standards.	Improved vetting accuracy, enhanced decision-making across research and administrative units, and strengthened institutional compliance with national research security requirements.	
UofT: Research Security Information Analysts	$357,925	Establish a sustainable, internal cybersecurity-as-a-service model at the University of Toronto to support researchers and academic divisions by implementing advanced protection, detection, and response controls.	Progress from baseline to target states in risk management, data classification, vulnerability remediation, and endpoint protection, as tracked by the Chief Information Security Officer.	Reduced cybersecurity risks to research, enhanced digital forensics capabilities, and a sustainable service model aligned with institutional cybersecurity priorities.	