University of Toronto – 2026-27 Research Security Fund – Institutional Performance Objectives

Project	Investment of Security Funds	Performance Objective	Performance Indicators	Target Outcomes	Reported Outcomes
Unity: Enhancing EDC Security/Resilience Through Migration from MySQL Community to MariaDB Community	$276,684	Strengthen REDCap security by implementing enterprise-managed authentication via Microsoft Entra ID, ensuring centralized identity governance and enforced multi-factor authentication.	Percentage of institutional users authenticating via Entra ID, number of environments migrated, MFA enforcement rate, and successful security/privacy approvals.	Full migration of institutional users to Entra ID with MFA, all environments federated, reduced local accounts, improved compliance, and streamlined identity management processes.	
UHN 1: Enhancing Web Security with Cloudflare	$62,708	Enhance web application security by implementing Cloudflare WAF, improving threat protection, availability, and access control across institutional research-facing web services.	Number of blocked threats, reduction in brute force attempts, percentage of traffic routed through Cloudflare, uptime metrics, and user access success rates.	Reduced successful attacks and login abuse, full traffic filtering via Cloudflare, improved service availability, and uninterrupted access for legitimate users across research platforms.	
UHN 2: Cloud Security: Zero Trust Network Access (ZTNA) for Unmanaged Devices	$72,930	Strengthen security by implementing Zero Trust Network Access for unmanaged devices, eliminating direct network access and enforcing identity- and role-based controls.	Percentage of unmanaged devices enrolled in ZTNA, reduction in related security incidents, policy compliance rates, and access restriction effectiveness based on user roles.	Majority of unmanaged devices onboarded to ZTNA, reduced incidents involving unmanaged endpoints, controlled application-level access, and improved visibility over remote device activity.	
UHN 3: Implementation of Data Loss Prevention Tool (Varonis)	$99,393	Improve data security posture by implementing Varonis DLP to automate classification, enhance visibility, and detect improper sharing of sensitive on-premises data.	Percentage of data classified, reduction in improper data sharing incidents, number of DLP alerts triggered, and trends in policy violations over time.	Majority of sensitive data classified, reduced improper sharing and breaches, improved audit readiness, stronger data governance, and enhanced visibility into high-risk behaviors.	
UHN 4: Migration from Armis to ORDR Platform	$45,160	Enhance network security by migrating to ORDR, improving device visibility, classification accuracy, and threat detection across all connected research and enterprise assets.	Percentage of devices migrated, reduction in unidentified or unmanaged devices, improvement in classification accuracy, and incident detection and response efficiency metrics.	Complete migration to ORDR, fewer unmanaged devices, improved device identification accuracy, stronger real-time visibility, and enhanced operational efficiency in monitoring and response.	

UHN 5: Migration to Microsoft Defender & Adoption of the Purview Suite	$339,001	Strengthen security and efficiency by consolidating endpoint, email, and data protection into Microsoft Defender and Purview, enabling unified visibility and control.	Percentage of endpoints and email systems migrated, number of legacy tools decommissioned, reduction in security costs, and improvements in detection and response times.	Full migration to Microsoft security suite, retirement of legacy tools, reduced costs, improved threat response, and enhanced data protection, governance, and visibility.	
UHN 6: Establishing Research Partnership Security & Compliance Capacity at UHN	$116,000	Strengthen institutional capacity to assess and mitigate research partnership risks by implementing standardized due diligence processes and dedicated compliance support resources.	Time required to review partnerships, number of reviews completed using SOP, adoption rate across teams, and milestone completion for tools and processes.	Standardized partnership review process implemented, reduced review timelines, increased consistency in risk assessment, and improved institutional awareness of research security requirements.	
Sick Kids: Research Security & Compliance Program	$601,773	Strengthen research security, compliance, and operational resilience through continuous monitoring, coordinated remediation, and integration of governance practices across Research IT environments.	Percentage of control gaps with active remediation plans, BC/DR coverage and testing rates, incident reduction, recovery time improvements, and compliance readiness metrics.	Reduced security and compliance risks, improved recovery readiness, sustained access to controlled datasets, strengthened governance, and established continuous compliance across research systems.	
Sunnybrook 1: Secure Research Network Expansion for AI-Enabled Clinical and Translational Research	121,178	Expand secure research infrastructure to support AI, genomics, imaging, and privacy-sensitive clinical research through scalable, compliant, and centrally governed platforms.	Secure storage capacity growth, number of research groups onboarded, utilization rates, reduction in non-compliant storage requests, AI project support, and user	Enhanced secure research capacity supporting AI, genomics, and clinical data; reduced non-compliant storage; improved governance, collaboration, and productivity. Strengthened privacy compliance, cybersecurity posture, and institutional readiness for	
Sunnybrook 2: Physical Security enhancement for research facilities	145,413	Enhance physical security infrastructure to protect research facilities, sensitive assets, personnel, and ensure continuity of critical research operations.	Reduction in unauthorized access incidents, percentage of facilities upgraded, response times to alerts, system uptime, and compliance with security standards.	Improved facility security and monitoring, reduced breaches and disruptions, stronger protection of research assets, enhanced compliance, and increased researcher confidence and safety.	
UT1: Advancing Secure Research Information Technology	500,000	Establish a dedicated secure research technology capability enabling compliant, scalable, researcher-facing security services, infrastructure, and support for regulated and sensitive	Number of researcher engagements, secure environments provisioned, System Security Plans supported, lifecycle integration points established, compliance readiness	Operational secure research capability with high researcher adoption, improved compliance readiness, scalable secure environments, integrated lifecycle support, reduced risk, and enhanced research competitiveness.	

UT2: Repository Platform AI Bot Traffic Mitigation and Service Stability Initiative	196,000	Improve repository security and resilience by mitigating AI-driven automated traffic through enhanced monitoring, traffic management, and automated response capabilities.	Service uptime, response times, support ticket volumes, automated workflows implemented, platforms integrated into monitoring, and infrastructure performance during high traffic periods.	Improved service stability and availability, reduced disruptions from automated traffic, enhanced monitoring and response capacity, and sustainable mitigation practices supporting secure, accessible research infrastructure.	
UT3: Advancing Research Security at the UofT	1,373,522	Strengthen institutional research security capacity through expanded advisory services, training, and tools supporting compliance, risk mitigation, and secure collaboration.	Number of training sessions delivered, risk assessments completed, researcher engagements, stakeholder collaborations, and utilization of due diligence tools across programs.	Expanded research security support, increased awareness and compliance, improved risk assessment coverage, stronger partnerships, and enhanced institutional readiness for evolving research security requirements.	