## *University of Toronto – 2022-23 Research Security Fund – Institutional Performance Objectives*

| Project | Investment of Security Funds | Performance Objective | Performance Indicators | Target Outcomes | Reported Outcomes |
|---|---|---|---|---|---|
| UT 1: Formal Launch of the UofT Research Security Program | Percentage of grant invested in supporting this project: 8.4% | To launch a Research Security program to guide and support members of our research community in planning and implementing their activities to continue to achieve maximum impact and minimize exposure to risks. | To hire a new Director, Research Security in the VPRI; dedication of staff time to new, incremental research security support activities; acquisition of essential tools and software to support the team; phased implementation of an internal process that helps members of the U of T community complete appropriate due diligence when they enter a partnership with any foreign | To hire a new Director of Research Security to establish a framework for managing geopolitical risk. | Our new Director of Research Security is now in place and is moving swiftly, with the support of other senior staff and academic administrators who have pivoted to work collaboratively, on establishing procedural framework for managing geopolitical risk. UofT is actively engaged in strategic conversations at national and regional tables. |
| UT 2: Replacement of Covered Equipment | Percentage of grant invested in supporting this project: 33.3% | To comply with U.S. National Defense Authorization Act on the use of "covered telecommunication equipment" as a "substantial or essential component" of any system. | Replacement of institutional network equipment that is non-compliant with section 889, Part B, of the U.S. National Defence Authorization Act, as part of a larger institutional IT security plan. | To replace all non-compliant equipment and ensure that the University has the capacity to prevent procurement from entities that threaten our eligibility with U.S. or Canadian government research sponsors. | All non-compliant equipment has been replaced and is fully operational. Procedures have been put in place, and will be further refined, to ensure that the University has the capacity to prevent procurement from entities that threaten our eligibility with U.S. or Canadian government research sponsors. |
| UT 3: Physical Security of Research Facilities | Percentage of grant invested in supporting this project: 4.9% | To provide enhanced safety and security for university research facilities. | To upgrade access control and to limit incidents of unauthorized access, theft and damage to research facilities | To complete all scheduled security projects for 2022-23. To prevent incidents of unauthorized entry and theft due to inappropriate access. | All physical security projects scheduled for 2022-23 have been completed. No incidents of unauthorized entry or theft due to inappropriate access have been reported. |
| CAMH 1: Research Biobank Database Application Upgrade and Compliance Configuration | Percentage of grant invested in supporting this project: 2.2% | Implement essential security measures for a valuable research asset. | Completion will be measured by the successful installation and configuration of the upgraded application, as well as time-to- | The installation of the upgraded application including database migrations. | Installation of the upgraded application was completed successfully, including database migrations. This upgrade enabled the configuration of additional |

| | | | | | |
|---|---|---|---|---|---|
| | | | completion for all tasks related to the compliance evaluation.<br>Key indicators: number of studies supported, number of biosamples, number of assays, number of regulated/non-regulated studies. | | security features, including two-factor authentication to ensure compliant authorization. |
| CAMH 2: Research Informatics Security Vulnerability Management | Percentage of grant invested in supporting this project: 1.5% | Reinforce cybersecurity through rigorous systems review and mitigation strategies using dedicated personnel. | Vulnerabilities are tacked using commercial software and monitoring tools into critical, important, moderate and low categorizations. These are also assessed for the time between identification and resolution (measured in days).<br>Key indicators: number of high/medium/low risk vulnerabilities resolved, number of patches applied, number of servers updated/upgraded, % rate <90 days / <60 days / <30 days to resolution. | To maintain cybersecurity posture by utilizing software applications. | Cybersecurity posture was maintained utilizing software applications to scan for and identify vulnerabilities. SmartScreen server tracking has effectively identified risks and reported these for action by Research IT to implement patches and updates. |
| UHN 1: Crowdstrike endpoint antivirus and detection | Percentage of grant invested in supporting this project: 2.2% | To implement CrowdStrike as the endpoint installed tool to provide monitoring and endpoint detection, thus aligning with the regional security operations centre. | KPIs are measured through regular threat scores that are generated via dashboards as well as reports that are developed internally and presented to UHN Boards. | Complete CrowdStrike implementation. | Implementation 100% completed on supported desktops and servers. |

| | | | | | |
|---|---|---|---|---|---|
| UHN 2: Variety of digital demands submitted by members of the Research community (20) requiring scope review by Digital Business Partner, Digital Operations & Digital Security Teams. Includes hardware and software purchase for operational cyber security. | Percentage of grant invested in supporting this project: .2% | Ensure that the scope, value, and expected timing of digital demands are assessed, and solutions are defined and effectively implemented. | Characterizations of the types of systems at risk.<br>Identifications of threats to those systems (unauthorized access, misuse of information, data leakage/exposure, loss of data, disruption of service).<br>Determinations of possible impacts of cybersecurity threats.<br>Identification of existing controls that may prevent, mitigate, detect, or compensate for potential threats.<br>Calculation of risk ratings based on combination of impact and likelihood of occurrence. | Develop controls to proactively prevent and/or mitigate risks. | A variety of efforts have been coordinated to prevent risks such as the UHN Digital Security Team conducted formal Threat Risks Assessments to analyze software or digital solution vulnerabilities. |
| UHN 3: Gigamon Project 3 year contract | Percentage of grant invested in supporting this project: 2.5% | Real-time views of East/West traffic within the environment, allowing threat detection to advance to a new level. | Number of malware applications detected and contained. | Implementation of the east/west firewalls | UHN has purchased Gigamon as a network tap solution for all of its network. With Gigamon, UHN Information Security gets real-time views of East/West traffic within the environment, which allows threat detection to advance to a new level. |
| UHN 4: Palo Alto Firewall project | Percentage of grant invested in supporting this project: 3.9% | Consolidating all firewalls into one product, Palo Alto, providing enhanced perimeter threat | Regular threat scores both through external services such as BitSight as well as internally generated data. | Implementation of the Research NextGen firewalls. | In this ongoing project, UHN is consolidating all of its firewalls into one product, Palo Alto. This will provide a much better perimeter threat detection service for all UHN, |
| UHN 5: Achieving QI and Enabling Research with REDCap | Percentage of grant invested in supporting this project: .7% | Centralize REDCAP management to meet organizational technical, privacy, and security | Number of research studies using REDCAP<br>User satisfaction and user experience. | Enhance infrastructure, operations and support of REDCap for the UHN research community; optimize end-to-end REDCap process workflows; migrating REDCap from HPC4Health to UHN | Implementation completed. |

| | | | | | |
|---|---|---|---|---|---|
| UHN 6: Research Devices Network Connection | Percentage of grant invested in supporting this project: 1.2% | Reduce vulnerability of data stored within research devices and create a new isolated network (VLAN) | Number of devices moved from the Untrusted Host or non-UHN domain to the UHN domain; number of devices with CrowdStrike and Nessus Agent installed; number of devices participating in the quarterly patching cycle; number of critical/high priority vulnerabilities outstanding on the devices without a security exception; number of devices connected to Comvault for automated backup services. | To migrate devices from Untrusted Networks to UHN Network; to install CrowdStrike and Nessus Agents on supported devices; to add backups to Comvault for supported devices. | Implementation is ongoing. |
| UHN 7: eSignature Rollout | Percentage of grant invested in supporting this project: .8% | Validate and implement an approved e-signature platform and process for electronically signing documents as part of a regulated process. | Increased adoption and usage of e-signature platform; Increased user satisfaction. | To validate and implement an approved e-signature platform and process for electronically signing documents (without PHI/CCI) as part of a regulated process. | AdobeSign implemented. |
| UHN 8: Proofpoint yearly fee | Percentage of grant invested in supporting this project: 1.6% | Run all incoming email through the Proofpoint filter to isolate spam/junk and malicious email. | Regular threat scores; internal reports; end user "click through" reports of test emails that are fraudulent to determine how well educational processes are working. | To purchase Proofpoint and implement as an effective email threat protection tool. All email coming in to the hospital is passed through our Proofpoint filter which isolates Spam/Junk and malicious email from a network tap solution for all of its network. | Implementation in process to have all email coming into the hospital pass through a Proofpoint filter which isolates Spam/Junk and malicious email. |
| UHN 9: Tenable Project, yearly invoice | Percentage of grant invested in supporting this project: 1% | Use Tenable to assess device and server vulnerability and provide continuous monitoring of all systems. | Regular threat scores generated via dashboards; Number of overall threats, especially from devices that are not computers. | To implement and maintain Tenable which is now in place for all UHN devices, whether research or not. This includes research device monitoring of end user computers as well as lab equipment (Mass Spectrometers, FLOW cell sorting, etc). Tenable has its own dashboard monitoring solution and in addition feeds our | KPI's are measured through our regular threat scores that are generated via dashboards as well as reports that are developed internally and presented to the UHN Board and Research Board of Directors. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | overall aggregate monitoring and threat detection tool Splunk. | |
| Sinai: Enhancing and Upgrading of Sinai Health's Research Cyber Security | Percentage of grant invested in supporting this project: 5.5% | Replace VPN server.<br>Install network access controller (NAC).<br>Upgrade and install a range of security software products. | Number of verified safe devices connecting to the network;<br>Number of uncertified devices recognized;<br>Number of potential/active threats identified;<br>Number of secure home computing devices. | Among other initiatives, to implement Microsoft Defender Plan 2 security product to greatly enhance edge level security at the end user level and stop threats before they arrive improving the security posture of the Institute. | Implementation successful |
| Trillium 1: Institutional Research Data Management (RDM) Strategy | Percentage of grant invested in supporting this project: <.01% | Establish measures, protections, and processes to ensure researchers access, use and share data appropriately and in compliance. | Established institutional RDM strategy;<br>Policy development and update;<br>Established RDM Privacy FAQ;<br>Established Data and Risk Matrix;<br>Central Data repository established. | To update policies and procedures to satisfy RDM requirements and support researchers with how to manage their data. | While ongoing, THP endeavors to ensure that data is being used securely and the appropriate considerations and security measures are being applied when working with the community's data. |
| Trillium 2: RCR/Integrity Framework and Practice Change | Percentage of grant invested in supporting this project: <.01% | Reframe and revitalize institutional research integrity/RCR education and culture | Gaps identified via engagement sessions data analysis;<br>Solution development through co-design;<br>Implementation and user testing;<br>Training and education. | Due to the pandemic, this work was placed on hold, as there were no dedicated personnel to help lift the work required to reframe and revitalize the institutional research integrity/ RCR education process. During the 2022/23 fiscal year, a Research Ethics and Compliance officer was hired to lead this work.<br>During the gap identification phase, the compliance officer noted that a number of other processes needed to be in place prior to the actual development phase. Following are a number of additional milestones underway that need to be met prior to the development stage:<br>Understanding how our landscape has changed over the last year and determining what other | The implementation of this project is underway. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | mandatory training would be required by our research community based on these changes (e.g. RDM requirements and training).<br>The development of our e-tools system: understanding how this can support revitalizing our RCR framework.<br>Ensuring the policies and procedures that guide our current research education requirements are up to date and captured appropriately.<br>Conduct an assessment to see whether additional information needs to be obtained from our research community prior to beginning the development stage. | |
| Trillium 3: Research Partnership Security | Percentage of grant invested in supporting this project:<.01% | Mitigate security risks in research when engaging in research partnerships. | Increased understanding of current practices, processes, and guidelines. | Develop, collect, and collate information and educational resources for researchers and staff towards helping protect the safety and reputation of TASHN as a whole and which will raise awareness of the potential risks associated with some external collaborations.<br>Seek to ensure a coordinated approach to the above, as well as clear points of contact for particular issues to avoid duplication of effort. | This project is currently ongoing with the development of joint principles and approaches for research partnership security for TAHSN hospitals |
| Trillium 4: Review, Assess and Prioritize eTools to Optimize Operations | Percentage of grant invested in supporting this project: .1% | Build a new electronic tool that will serve as a real-time enterprise management system. | Completion of the e-Tool(s) research operations enterprise management system.<br>Percentage of efficiency achieved by the deployment of the tool. | The e-Tool(s) Research Enterprise Management Solution will provide a one stop electronic solution for managing all research operations and innovation activities at THP/IBH. This will ensure that all research operation and innovation activities are performed and tracked in a single secured platform. | While in progress, the outcomes of this project will enable the following units to work with increased efficiency. It will directly inform and support their core and cross-functional requirements during regular operations. |

| | | | | | |
|---|---|---|---|---|---|
| Trillium 5: Data Platform Development | Percentage of grant invested in supporting this project: <.01% | Manage security risk for AWS platform. | Implement AWS Control Tower for platform management;<br>Achieve CIS benchmark compliance; | To successfully deploy an AWS Control Tower to manage AWS environment. This service automates the setup of a well-architected multi-account AWS environment, ensuring a secure, compliant, and scalable foundation for our | AWS Control Tower has been successfully deployed/ |
| Trillium 6: Update and Revalidations of all Legal, Liability, Privacy and Security | Percentage of grant invested in supporting this project: <.01% | Review and update all agreement and contract templates to meet new legal, risk and privacy | Number of updated templates and SOPs;<br>Number of new templates created to support the functional area | Our current suite of agreements, contracts, templates and standard provisions was developed a few years ago and therefore requires a detailed review and update to comply | While ongoing, the outcome of the project has included the update of an existing suite of tools and the creation of new ones, this is to |
| Trillium 7: Corporate Research Risk and Privacy Management and Quality Assurance | Percentage of grant invested in supporting this project: <.01% | Ensure all contracts and agreements meet with all security and privacy requirements. | % of project, agreements and files where we mitigated security and/or privacy risks;<br># of Projects, Contracts and Agreements with mitigated security and/or privacy risks;<br>Frequency of flagged and | As studies become complex with a web of partners and collaborators using different system and tools, the need for a robust review process to identify and mitigate privacy and security threats become extremely important. | The outcome of this project has positioned the department to flag security and privacy risks that has further helped us to support different functions in the hospital. This has positively impacted on our relationships with key stakeholders. |
| Baycrest 1: Installation of Endpoint Detection and Response Software | Percentage of grant invested in supporting this project: .3% | Implement endpoint detection and response software to improve institutional security posture. | Increased number of institutional endpoints with new software; target > 80% coverage by end of March 2023. | The successful installation of Endpoint Detection and Response software which is recognised by the IT industry as the current standard in computer security measures. In addition, cyber-insurers are requiring a certain percentage coverage of business assets to be covered by an approved EDR product as a prerequisite to offering insurance coverage. | Actual Results: EDR software has been deployed to approximately 80% of computer endpoints in use at the Institute throughout the summer of 2023. Although rapid-deployment tools were used to assist with installation and configuration of this software on the first 50% of our asset pool, the second half of the pool required lengthy operating system upgrades (several hours per computer). The impact of this heavy workload has had important impacts on IT operations, for which additional resources are essential. Deployment is progressing according to schedule, with a further 10% deployment rate (90% |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | in total as required by our cyber insurance provider) expected in Fall 2023. |
| Baycrest 2: Upgrade of Virtual Private Network (VPN) License | Percentage of grant invested in supporting this project: .2% | Upgrade the VPN concentrator to bring VPN encryption levels up to modern standards. | Full update and install to concentrator module and/or hardware firewall | VPN is the technology used by staff who are working from home, a mode of employment duty fulfillment, which has become more popular in the aftermath of the COVID-19 pandemic and resulting lockdowns. This is especially applicable for those who have been instructed to self-isolate, but also apply to those duties warrant working from home as a form of prophylaxis.. In a bid to mitigate risks, cyber insurers are requiring up-to-date networking technology on both the hardware and software fronts, of which VPN tools are members. | Actual Results: the institute's VPN module was ordered and is being configured. The upgraded VPN allows for much more secure inter-site connections for both our offsite staff as well as remote vendor hardware monitoring service as required by our high-complexity neuroimaging technologies. Certain such vendors have advised us that |
| Baycrest 3: Upgrade of Network Switch for Baycrest Central Registry | Percentage of grant invested in supporting this project: <.01% | Upgrade network switching equipment to improve protected health information security held by the client registry system. | Conversion of existing firmware-defined network segmentation into full hardware-level segregation. | Network segregation is recommended to isolate systems containing sensitive data from those not requiring access to these data. Workloads can be separated on a "need to access" basis. Through limiting access to sensitive areas, overall exposure to security risks is reduced. | Actual Results: Equipment has been installed and will go live when system is fully activated. |
| NYGH: Raising Awareness of Research Security at a Community Hospital | Percentage of grant invested in supporting this project: .2% | Raise awareness of potential security risks among researchers, perform an internal risk profile audit, and implement processes to reduce risk. | Awareness of issues related to research security. | We assembled various guidelines produced by agencies of the federal government and their counterparts in the United States and provided an orientation to the NYGH research community. | The initial level of awareness among this group was low and it has improved since. We updated the corporate policy on the treatment of intellectual property. We also updated safeguards for managing access to the physical space for research and computer network. |

## *University of Toronto – 2022-23 Research Security Fund – Institutional Performance Objectives*

| | | | | | |
|---|---|---|---|---|---|
| SRI 1: Cybersecurity Infrastructure Updates for SRI and Threat Detection and Preventative Maintenance | Percentage of grant invested in supporting this project: 4.7% | Install CrowdStrike on Linux and specialized equipment, and proactive vulnerability assessments and remediation of potential cyber threats. | Number of potential threats detected. | Successful implementation of updates and maintenance. | Security analyst deployed advanced antivirus applications on Sunnybrook Research Institute Linux, Mac and Windows machines. Proactively monitoring and scanning activities were completed as well as threat detection and remediation activities. Major upgrades of common research applications for clinical data (REDCap) completed in |
| SRI 2: Upgrades to Current Security Infrastructure Access Controls | Percentage of grant invested in supporting this project: 1.9% | Expand current security infrastructure and update access control system. | Number of new card readers<br>Number of additional cameras | Successful implantation of upgrades. | In endeavouring to complete the Research Security project at the Sunnybrook Research Institution, the institute procured additional |
| HSC: Research IT Cyber Security Personnel and Licenses | Percentage of grant invested in supporting this project: 13.1% | Assessment of current procedures, rollout of new cyber security policy, and ensuring principles are included in research data management strategies. | Hiring, training, and integration of new Senior Information Risk Analyst; number of risk assessments performed. | Putting in place a Senior Information Rish Analyst. | The Hospital for Sick Children put together a call for a Senior Information Rish Analyst. This search was successful in identifying a suitable candidate and thus a Senior Information Risk Analyst has been hired and trained. To date, three risk assessments were performed on new contracts |
| Unity 1: Research Cyber Security Initiatives and Measures | Percentage of grant invested in supporting this project: 3.9% | Protect IT security and data in the research environment. | Number of simulated phishing attempt tests;<br>Number of potential/active threats detected;<br>Number of vulnerability tests on specific computers/users. | Successful implantation of project and security measures. | Countless security measures were completed such as simulated phishing attempts across Unity that were available to all nearly 2,000 research personnel, as well as active endpoint detection for all Unity Health managed digital devices such as laptops. This level of active monitoring and surveillance is integral for maintaining cybersecurity of research environments. |

*September 2023*

| | | | | | |
|---|---|---|---|---|---|
| Unity 2: IT Security Specialist and Associated Personnel to Assist with Research Security Assessments | Percentage of grant invested in supporting this project: 1.4% | Provide threat and risk assessments during data projects and construction of cyber secure databases. | Number of threat and risk assessments conducted. | Identification of potential threats and risk assessment. | Any projects that met the criteria for needing Unity Health's requirement for needing a threat and risk assessments were completed. Threat and risk assessments ensures that proposed research has the security compliant infrastructure prior to the launch of projects which adds a layer of protection to projects prior to their inception. |
| Unity 3: Physical Security Measures | Percentage of grant invested in supporting this project: 2.9% | Ensure a safe and protected research environment by assessing physical security of people, assets, data, and research animals. | Number of assessments and reports generated. | Successful implantation of project and security measures. | Unity Health Research has been integrated into the security monitoring reports for the whole organization's digital operations. For example, research digital assets that are monitored are integrated into the overarching Unity Health Toronto's Security Information and Event Management (SIEM). This provides one enterprise wide view for security operations and adopts the best practices of the hospital that is fully equipped to handle the most sensitive and confidential patient health information to all levels of integrated research assets. |
| Holland Bloorview: Optimization of Research Security Through Enhancements and Leveraging Resources | Percentage of grant invested in supporting this project: .8% | Enhance on-premises research security processes by leveraging existing information security infrastructure | Number of hours spent by technical personnel on integration. | Successful optimization of Research Security through integrated enhancements. | Our technical personnel successfully integrated the research network into the hospital infrastructure that adopted all of the security protocols from the hospital e.g., network monitoring, intrusion detection, |

| | | | | | |
|---|---|---|---|---|---|
| | | employed across the hospital. | | | firewalls. By working closely with the hospital IMT staff, our technical personnel ensured the appropriate technology solutions were applied across the research network. Once integrated our technical personnel managed user permissions, resource deployment and cloud configurations for research labs ensuring research data and audit trails are appropriately maintained, secured, and backed up. Also ensuring the confidentiality of research data across. |