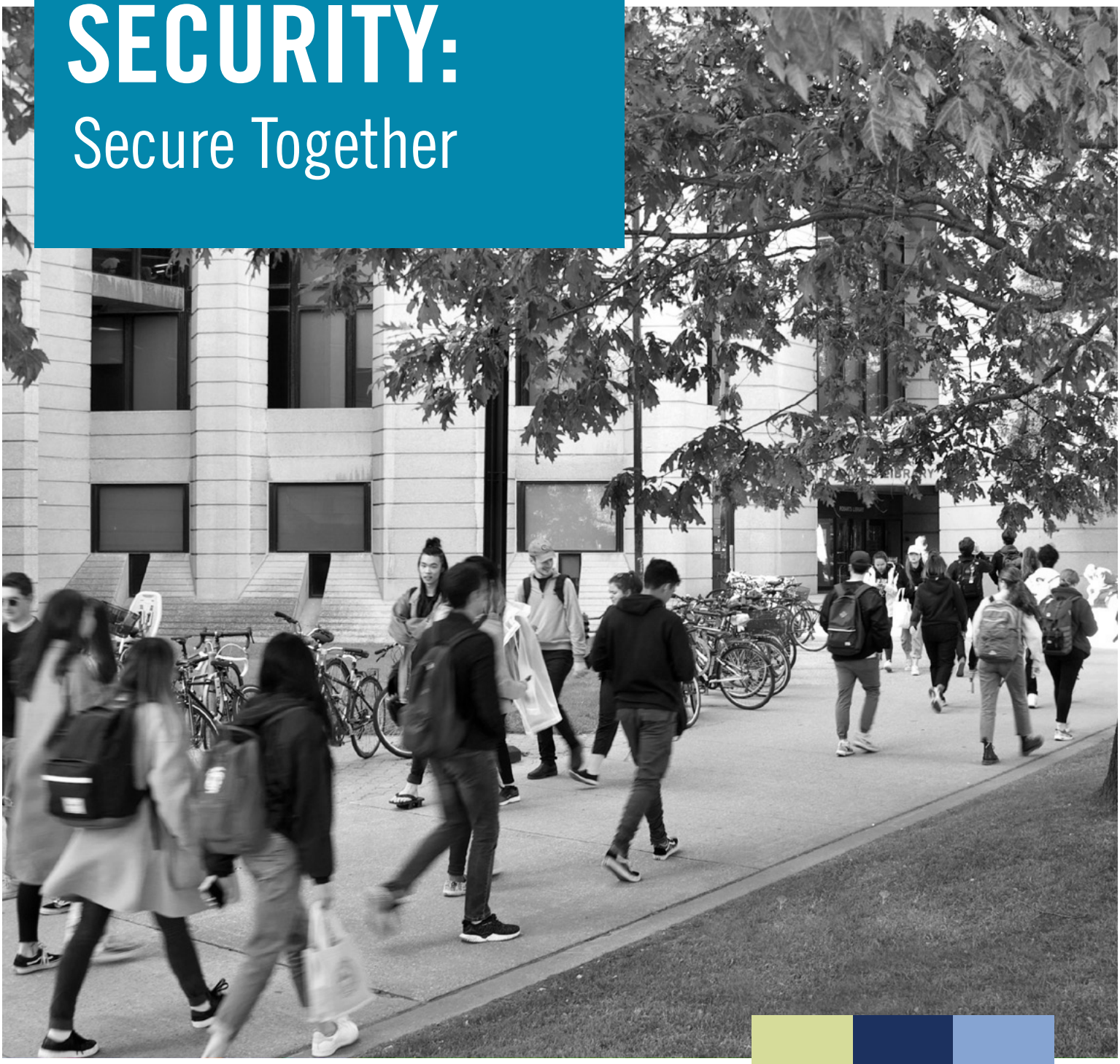
INFORMATION SECURITY:
Secure Together

Annual Report
May 2022 – April 2023



UNIVERSITY OF TORONTO

SECURE of TOGETHER

Table of contents

Introduction	3
Key risks and highlights	4
Success stories from across the tri-campus community	6
What lies ahead	12

Introduction

This annual progress report highlights the risk and achievements of the University of Toronto's tri-campus information security program for the 2022 – 2023 fiscal year.

The year 2022 – 2023 introduced new security risks and challenges but also created unique opportunities. The geo-political situation amplified the information security risk to the University, making it critical to act quickly and with purpose. At the same time, we saw an increased return of faculty and students to campus and with that a continuing need for secure digital transformation. In the aftermath of COVID-19, hybrid work is no longer a response to the pandemic but a reality of how we teach, learn, and research.

In this report, we have highlighted the great work that is happening both at the institutional level and within divisions. Success stories from across the tri-campus community continue to demonstrate that we truly are **Secure Together**.

We faced the challenges head on, and we are better for the experience. However, there is a lot more that needs to be done. The risk continues to grow, and it is important that we vigilantly mitigate risk with a bias for action. The only way we can protect our people, our data, and our systems from increasingly sophisticated and potentially crippling security threats is by coming together to make real and lasting change.

> "We have an obligation to protect our people, our data, and our systems from increasingly sophisticated and potentially crippling security threats."
>
> **Isaac Straley,**
> Chief Information Security Officer, U of T

Key risks and highlights

Highlights

Enabled multi-factor authentication for **100 per cent** of appointed staff, faculty, and librarians and **100 per cent** of students

UTM deployed next generation anti-virus for **2,000** endpoints

UTSC improved its **ransomware preparedness** by documenting and testing its security incident response plan

90 per cent of target academic and administrative divisions completed the data inventory and risk self-assessment

Led a community-driven, tri-campus effort to define the **information security strategy** for the University

Key security risks

1. **Remote work:** Post-pandemic, hybrid work is a reality of how we teach, learn, and research. This means people, devices, and data need protection wherever they are.
2. **Ransomware:** Risk of ransomware continues to rise with attackers becoming more sophisticated and targeting research and education institutions.
3. **Fraud and phishing:** Community members, specifically students, are frequently targeted in a range of fraud schemes through phishing and other means. Phishing continues to be one of the most effective methods to perpetrate data breaches.
4. **Attacks targeted at researchers:** Researchers are at risk from sophisticated attacks, espionage, and foreign interference activities. Geo-political tensions have further aggravated this risk.
5. **Supply chain:** We rely on third parties for many critical services, including hosting and processing of sensitive data. Security incidents or vulnerabilities impacting our suppliers put the University at risk.
6. **Data governance:** Copies of data in unknown or under-protected places increase the likelihood of data theft and inappropriate data exposure. This also increases the impact of ransomware attacks.
7. **Compliance risks:** The University is obligated to meet regulatory and contractual requirements such as the Payment Card Industry credit card protections. Expect increased requirements from research sponsors.
8. **Denial-of-service attacks:** The research and education sector in Canada has seen an increase in cyber attacks designed to cripple operations and impact availability of services.

U of T information security strategy

The Office of the Chief Information Security Officer launched a tri-campus effort to build the information security strategy for U of T. The strategy aims to provide a shared direction and approach for shaping the evolution and growth of information security and privacy at the University.

A community-driven approach was followed involving extensive consultation with academic and administrative units across the University. Here are the themes and ideas that evolved from the consultation.

Objectives

Secure University digital transformation
Ensure security and privacy is at the core of emerging technologies and new ways of teaching, learning, and working adopted by the University.

Trustworthy teaching, learning, and research
Enable structures to ensure scholars, researchers, academics, and staff feel safe when using University infrastructure, systems, and resources.

Resiliency through effective risk management
Strategically assess and manage risk to prevent security attacks and minimize their impact through timely detection and response.

Excellence through collaboration
Harness the power of partnerships to solve bigger and more complex challenges.

See the full strategy here.

Strategic goals

1:
Enable the mission of the University

2:
Uphold privacy, openness, and free inquiry

3:
Deliver a world-class, exemplary information security program

Success stories from across the tri-campus community

Securing the University's digital transformation

Endpoint protection – U of T Mississauga's deployment

Increase in remote work and the heightened risk of ransomware attacks has amplified the need to protect endpoints such as servers and end user devices. Traditional anti-virus is no longer sufficient against sophisticated attacks and next-generation capability is needed for timely detection and response.

UTM successfully deployed next-generation anti-virus to over **2,000** endpoints and paved the way for adoption of the capability for the rest of the University. **UTM is now an active partner in rolling out the capability at the institutional level**, providing the benefit of its experience to accelerate the initiative.

> "The next-generation anti-virus deployment at UTM has been a resounding success, providing unparalleled protection against malware and other security threats. The deployment has helped UTM to strengthen its security posture and has contributed significantly to the tri-campus initiative by providing a blueprint for endpoint security. It has demonstrated the potential for next-generation anti-virus solutions to enhance security in higher education. UTM is proud to be at the forefront of this critical technological advancement."
>
> **Anthony Betts**
> Director, Information & Instructional Technology Services, UTM

Institutional endpoint protection effort

The institutional rollout of next-generation endpoint protection, co-led by ITS Information Security and UTM, has garnered support from multiple units across the tri-campus community. So far, Arts and Science, UTSC, KPE, Pharmacy, Medicine, EIS, and Music have signed up for the pilot. At least 32 units have indicated interest to participate in phase two of the rollout commencing in May 2023.

Licences
2,000
Available licences for pilot

Endpoints
1,076
Endpoints provided so far for pilot

Onboarded
826
Endpoints onboarded for early pilot

Multi-factor authentication

We can proudly say that the entire University community, with a few exceptions, is now MFA-enabled — the single best protection against compromised accounts. It was a long and strenuous journey, but we are finally here, and most importantly — we did it together.

This has been a true tri-campus effort with the ITS Information Security team coordinating the deployment and divisions spearheading engagement and communication to faculty, librarians, staff, and students.

Key highlights

Enabled for **100 per cent** of appointed staff and faculty

Enabled for **95 per cent** of non-appointed staff

Enabled for **37 per cent** of adjunct faculty

Enabled for **100 per cent** of students

"The MFA onboarding of faculty and staff at Engineering was made possible thanks to the engagement and support from the academic leadership from each department, and the excellent collaboration of IT staff across the faculty who supported our clients."

Alex Tichine
Director, IT, Faculty of Applied Science and Engineering

"It's been a pleasure working with Haniyeh, Deyves, Arathi and the team at Information Security on the rollout of UTORMFA to students. Their organization and troubleshooting helped to ensure this process was smooth for students, and their planning, in collaboration with the tri-campus help desk teams, helped to make this rollout a success."

Jessie Metcalfe
Assistant Director, Office of the Vice-Provost, Students

Modernizing data access: Journey with Kinesiology and Physical Education

The Faculty of Kinesiology & Physical Education partnered with the ITS Information Security team to enhance access controls for various systems (both enterprise and local level) via the UTORGrouper service.

Key highlights:

- Enabled role-based access management for applications like SharePoint libraries, shared email addresses, and other local and enterprise-level applications
- Increased the efficiency and consistency of the onboarding and offboarding process
- Streamlined application access based on pre-defined roles and permissions

"In 2023, KPE will continue to work with HR and IS to link Grouper with HRIS to automate the assignment of role-based access and eliminate the manual process of assigning access to individuals. This will further increase efficiencies in access management, reducing the risk of unauthorized access across KPE."

Paul Morrison
Director, Information & Instructional Technology, Faculty of KPE

New UTORGrouper features:

- Web interface response improved
- Synchronization time for access groups reduced to five minutes from two and a half hours
- Paved the way for integration with Enterprise AD and Azure AD services

Identity improvements at Student Life

Student Life integrated more applications with their in-house identity system to streamline and improve their user onboarding and offboarding process.

"With the enhancements we made, the access request process for new joiners has become a simple and quick task. Our goal is to further streamline onboarding and offboarding by implementing and advancing our tools. We will also focus on building an information security awareness program for staff and faculty to enable more informed decisions."

Do Anh Vu
Associate Director, IT, Division of Student Life

Enabling safe and trustworthy teaching, learning, and research

Data management guidelines

The Institutional Research & Data Governance team led a cross-functional working group with expertise in privacy, information security, IT, records retention, and data governance to develop the data management guidelines that will be rolled out to staff in 2023.

These guidelines:

- Enable data-informed decision making by managing data as strategic assets
- Promote common understanding and consistent practices for data management
- Inform about related standards and guidelines from information security, privacy, data governance, and records retention

> "The guidelines serve as a high-level guide to assist U of T administrative staff in applying consistent approaches to the management of institutional data throughout their lifecycle. These guidelines aim to identify recommended institutional processes, tools, and available resources, along with clarifying key roles/responsibilities associated with the management of these data."
>
> **Jeff Waldman**
> Manager, Institutional Data Governance

Security protections for the Microsoft 365 environment

ITS implemented critical security features to U of T's institutional email and collaboration tools in M365 as part of the continuous improvement lifecycle required to maintain a trusted platform. These protections cover 100 per cent of active faculty, librarians, staff, and students who use M365.

New features:

- Reduction of malicious content via Safe Documents, Safe Attachments and Safe Links
- Anti-impersonation controls to highlight scam emails
- Detection of compromised accounts using Defender for Identity

Preventing fraud to create a safe community

The University of Toronto's Tri-Campus Fraud Prevention Working group was established to address concerns about community members, specifically students, being targeted in a range of fraud schemes. Over the course of the past year, the working group has developed a comprehensive communications framework to disseminate prevention education, training and strategies to all members of the University community.

Key achievements include:

- Train-the-trainer model for residence dons, enabling them to educate students living in residences.
- Fraud Prevention Squad, a peer-to-peer education model empowering students to spread awareness among the student community.
- Resources and brochures available in six languages (Arabic, Hindi, Russian, Simplified Chinese, Spanish, and Traditional Chinese) to expand outreach.

Bridging researcher needs and information security requirements

Sponsors are increasing research security requirements, affecting both researchers and supporting offices across the University of Toronto. The Research Information Security Program has partnered with the Office of the Vice-President of Research & Innovation and the Office of the Vice-President International to build a unified approach to support our scholars. These efforts include:

- Drafted easy-to-understand guidance documents and training resources to increase the autonomy of, and reduce burdens for, researchers
- Advised research-focused units on security and privacy protections
- Built relationships with researchers and support staff
- Worked on a framework for trusted digital research infrastructure

Resilience through effective risk management

Risk management journey highlights at academic divisions

Department of Computer Science (Faculty of Arts and Science):

- Increased resilience to security attacks by documenting its Information Security Incident Response Plan.
- Protected its teaching lab workstations against password theft by implementing anti-keylogger protection.

"In 2023, we will test out our new incident response plan for effectiveness and accuracy. The work that we undertook has improved the department's ability to address information security threats, providing a more secure environment for students, staff and faculty."

John Di Marco
Director, Information Technology, Department of Computer Science

Pharmacy:

- Adopted the ITS vulnerability management tool which led to the identification and remediation of over 380 vulnerabilities.
- Successfully deployed ITS-supported next-generation anti-virus on servers, research workstations, and staff computers containing sensitive data as part of the institutional endpoint protection pilot.
- Migrated all shared data to the institutional M365 platform, bolstering staff and faculty resilience against ransomware and preparing for a migration to Azure Active Directory.
- Strengthened the security team by recruiting Manager of Information Systems Security with a dotted line to the CISO.

"Moving forward, the Faculty of Pharmacy aims to enhance information security in their research labs through security awareness campaigns, integration of UTORMFA for research personnel, and network segmentation and segregation."

Adam Trent
Director, Information and Learning Technology, Pharmacy

University of Toronto, Mississauga:

- Implemented a vulnerability management program to regularly scan data center assets and mitigate risks from open vulnerabilities through a custom remediation workflow built into UTM's service management system.
- Established a process, in collaboration with the procurement team, to include formal third-party risk assessments for all applications procured through an RFP process.
- Rolled out next-generation anti-virus solution across all their managed infrastructure, which is approximately 2,000 servers, laptops, and desktops.

"In 2023, UTM will focus on expanding the scope of its existing projects and introducing new initiatives to provide a safe and secure IT environment for its students, staff and faculty members."

Akshat Mishra
Information Security Program Manager, UTM

University of Toronto, Scarborough:

- Developed an incident response plan and ran an in-house ransomware tabletop exercise, with plans to partner with Information Security to institutionally expand tabletop exercises in 2023.
- Completed third-party risk assessments enabling project teams to make more risk-informed decisions.
- Increased unit participation in the DAI-IRSA program, identifying risks and security process and technology gaps and focusing efforts to address them.

"The UTSC Information Security team has been using DAI-IRSA results to collaborate with participating units in reducing risk across UTSC and the wider University community."

Romel Sargezi
Information Security Analyst, UTSC

Coming together to tackle Log4j

On Dec. 9, 2021, a new high risk security vulnerability called Log4j was uncovered. The vulnerability was ubiquitous and easy to exploit. Tackling this threat required the community to come together in new and innovative ways and that's exactly what we did.

Steps taken to address log4j:

- Created tri-campus communication channels for collaboration on the response and sharing of threat intelligence and guidance.
- Proactively blocked suspicious network traffic.
- Shared indicators of compromise with other higher education institutions through CanSSOC and CIRA DNS shield.
- Continuously looked for signs of possible compromise.

As a result of the effort, the tri-campus team identified and protected 17 devices that were being targeted by threat actors using the Log4j vulnerability. This shared effort was recognized and won the 2022 Exemplary U of T Ambassador Award.

Response to U.S. Section 889

The enactment of the U.S. National Defense Authorization Act (NDAA), Section 889, paved the way for increasing supply chain risk management, empowering information security experts to better advise on risks when purchasing equipment and services. It also highlighted the importance of the university network as a shared strategic asset requiring more common practices and management.

Excellence through collaboration

Collaboration across the tri-campus community

The University depends on a collaborative approach for risk management. We continue to find better ways for distributed teams to align and deliver.

- **Shared governance with the Information Security Council:** The ISC, with strong representation from faculty, librarians, and students, ensures the CISO and unit heads are accountable to properly prioritize risks and mitigations.
- **Shared leadership:** Divisional representatives are stakeholders in decision-making processes for key security initiatives.
- **Engagement on security matters:** The community frequently comes together to discuss security matters through forums such as the Tri-Campus Security group, Active Directory Security Forum, and Coffee with the CISO.

"I joined U of T two years ago and was encouraged to attend the weekly Tri-Campus Security meetings. This is where I was introduced to several security topics such as MFA and vulnerability management. The interactive discussions provided insights for my own projects and allowed me to connect with subject matter experts on multiple topics. These meetings opened my eyes to the importance of information security and led to my transition to the role of Information Security Manager at Pharmacy."

Byron Qu
Manager, Information Security, Pharmacy

Sector leadership

We have continued to build strong partnerships across the sector and contributed to addressing shared security challenges.

- We have supported the ongoing evolution of CanSSOC and its integration with CANARIE to build a national approach to cyber security that benefits the whole sector.
- The CISO represented U of T on the Broader Public Sector cyber security expert panel. The panel provided recommendations to improve cyber resilience which were fully accepted by the government.
- We partnered with the Ontario Ministry of Public and Business Service Delivery to host a student-centric event to promote cyber security careers.

"U of T is a key partner to CanSSOC, a collaborative cyber security initiative that's building a trusted community to detect and respond to cyber security threats facing Canada's research and academic institutions. Working together, we are driven by a common vision to strengthen the cyber security capacity, capability, and maturity of the sector."

Jill Kowalchuk
Senior Director, CanSSOC Services, CANARIE

Capture the flag student event

The Office of the CISO provided support for a student-led capture the flag event to teach cyber security skills to students. This was a collaboration between U of T's capture the flag team, the Google Developer Student Clubs, and Mathematical and Computational Sciences Society, with support from other partners including Information Security.

"This was one of the most exceptional and memorable experiences I've had. The challenge required a unique combination of technical skills and critical thinking that kept me engaged and challenged throughout the entire experience. The fact that the challenge was based on real-world scenarios made it all the more immersive and enjoyable."

Capture the flag participant

Key highlights:

- 23 unique cyber security challenges based on real scenarios
- High turnout of 57 teams and 134 players
- Over 20 per cent first-time participants

Competing on the science while collaborating on protecting data and researchers:

U of T and McMaster met with key stakeholders from research intensive universities who agreed on the principle to support one another in meeting information security requirements, while retaining their competitive edge. This led to the creation of the CUCCIO Research Information Security Special Interest Group (SIG) representing 10 Canadian research-intensive universities. The group met for the first time in January 2022 and took the following steps:

- Discussed unique security concerns faced by researchers and how Canadian institutions can collaborate on safeguarding research
- Initiated sharing of in-house information security resources to reduce the burden on individual institutions

What lies ahead

Our shared vision is to expand our strong foundation to navigate ever-changing risk, enable digital transformation, and support tri-campus units as they focus on discipline-specific priorities.

The risk continues to change at an unprecedented rate and there is still a lot to do. Progress requires collaboration, hard work, transparency, and a genuine desire to see the best for the University.

Information security work does not happen in a vacuum – IT staff must keep the lights on and continue to deliver new features, all while trying to increase trust and resiliency of digital platforms. Yet, the work goes beyond IT. Everyone helps ensure the security of our data and the safety of our community – from being vigilant to phishing messages, to updating devices, and handling data thoughtfully.

Looking ahead, we have many exciting improvements planned to ensure that, as we increase our security posture, we also enable the mission of the University. Some of these improvements will be to tri-campus, institutional services and platforms. But much of the work will happen within divisions, departments, and research labs as they are best positioned to understand what is needed and what works.

Great information security is not technical or transactional, it is transformational.

Key focus areas

Build a security-aware culture by providing curated and contextual information security and privacy training, and simulated phishing exercises.

Drive development of divisional risk management programs signed off by the unit head and reviewed by the Information Security Council.

Reduce risk to critical assets and endpoints through expansion of next-generation anti-virus protection and proactive identification, tracking and reporting of security vulnerabilities.

Drive national priorities through continued participation in CanSSOC, especially through RIG Innovation Program, supported by 14 leading Canadian research universities.

Office of the Chief Information Security Officer

University of Toronto
Simcoe Hall
27 King's College Circle, Room 5E
Toronto, ON M5S 1A1, Canada

ciso@utoronto.ca | Tel: 416-978-7857
security.utoronto.ca

UNIVERSITY OF TORONTO