Approved Minutes (PV)

Meeting:	**Information Security Council - Meeting**
Date & Time:	**Tuesday, March 28, 2023 (10:00 – 12:00 P.M.)**
Location:	**HYBRID: The School of Graduate Studies, Room 101, 65 St. George Street, Main Floor/via MS TEAMS**

CHAIR:

Deepa Kundur

ATTENDEES:

Luke Barber, Rafael Eskenazi, Dimitris Keramidas, David Lie, Alex Matos, Sian Meikle, Aidan Mitchell-Boudreau, Andrew Petersen, Zoran Piljevic, Isaac Straley, Bo Wandschneider

BY INVITATION :

Sotira Chrisanthidis, John DiMarco, Deyves Fonseca, Kalyani Khati, Sue McGlashan, Paul Morrison, Kanupriya Parab, Jaro Pristupa, Carrie Schmidt

REGRETS:

Tero Karppi, Rohith Sothilingam

NOTE TAKER:

Andrea Eccleston

Item #	Item	Discussant	A	E	I
1	**Welcome:** The meeting convened at 10:10 p.m. with co-chair Deepa Kundur presiding. The Chair welcomed members and guests and called the meeting to order.				
2	**Approval of agenda:** **Motion:** The Chair invited comments from the Council regarding the Agenda. The ISC agenda of March 28, 2023, was approved as presented. **All in concurrence**				
3	**Approval of minutes:** The Chair invited comments from the Council regarding the Public and Full versions of the ISC minutes. **Motion**: To approve the Public and Full Minutes of February 27, 2023, ISC meeting as presented. **All in concurrence**				
3	**CISO updates:** Isaac S updated the Council on changes to the monthly IS Dashboard, noting that the purpose is to improve the level of details on measurements related to metrics such as risk and security. He said that a second dashboard will also be distributed to principals and deans to highlight key measurements in the academic space. The reports will be available to a limited audience. The Council was also updated on the following initiatives: **Endpoint Protection**: ➢ Isaac S provided data points on the number of departments participating in the pilot program. It was noted that the goal is to evaluate the software, address two major areas and document the privacy piece to ensure transparency.				

	MFA: ➢ Noted that 100% of students are now enrolled. He said that work also underway to resolve the ongoing issues related to some adjunct faculty. **Security Awareness Training**: ➢ Have selected a vendor, ORION. ➢ A pilot is underway, and the plan is to onboard 10,000 staff in the first year. **Vulnerability Management:** ➢ A contract staff is currently on board. He also noted improvement in unit-based reporting.
4	**UofT Information Security Strategy:** Kalyani K. presented the Info Security Strategy for the Council's endorsement. She noted that a strategy is needed as the UofT is highly decentralized when it comes to the managing of security, shared responsibility, and accountability. She noted that the goal of the strategy is to supply a shared vision and provide units with the opportunity to build risk management programs. In terms of the process noted that this was a Tri-Campus effort. Extensive consultation with units across the university was done to define a 4-year strategy and identify key initiatives at the institution level. In terms of execution, this will be released in two phases. It was also noted that the CISO will further consult with the ISC on the rollout plan and the approach for operationalizing the strategy. The Chair noted that this is an important initiative given the geopolitical situation and general funding. She added that it is important that we demonstrate our ability to manage risk from multiple perspectives, including the research setting. **Discussion Points:** ➢ The strategy has been socialized, and the community is aware of these initiatives, so there should be no surprise. ➢ The prioritization model will be provided to the community so that they can use it to define their priorities during their planning process. ➢ Need to include how much change management would be needed in terms of resources on a timeline. ➢ Also need to consider the complexity as some of these initiatives like Endpoint could be politically difficult for a segment of the university. ➢ A suggestion was made to add "currently" to item C of the request for endorsement. ➢ Need to establish some structure around implementation and alignment in the operational plan with division, such as a Customer Advisory Board. **Endorsement:** **The Chair moved to endorse THAT the** Information Security Council endorses THAT (a) the Information Security Strategy sets the strategic direction for information security at UofT. (b) progress against the strategy will be tracked and reported. (c) the ten institutional initiatives identified in the strategy will be prioritized. (d) units will identify their security priorities and operationalize execution plans. AND (e) ITS Information Security team will drive the ten institutional initiatives outlined in the strategy. **Motion** approved with the modification to add "currently" to item C. **All in concurrence**
5	**Additions to Information Security Control Standard: 40:35** Deyves F provided an overview of the Information Security Control Standard. He noted that a proposal was made to update the control standard based on the number of factors. - Controls are needed to protect our digital assets.

	- To increase our ability to meet security requirements set by research sponsors. Noted that consensus could not be achieved on the applicability of 1 control, which has resulted in a split in the language. ➢ Majority opinion is the control should be "required" and ➢ The minority opinion is that the wording should be "recommended" with respect to the local MFA for local administrative access, not the remote access. The members representing the minority opinion for wording to be "recommended" provided the Council with their concerns about what level 3 data is in term of how it is used in academic teaching and the impact this would cause to this segment of the university. **Discussion Points:** ➢ Isaac S clarified that CMMC is based on the NIST800-171 standard that will apply to all U.S. funded research for "Controlled Unclassified Information," which makes up a large portion of the UofT's U.S. research dollars. Most U.S. universities are *adopting* the CMMC and we chose to *align* (where reasonable) to this framework to support the University's strategic aim to increase funding from U.S. (and other international) sources. ➢ There is some value in setting a target when it is an achievable target. Need to have some parameters to measure against and our capability to meet the standard. ➢ Can the issue be addressed at the point of access with MFA? ➢ Need a broad way to address our information security requirement to meet both research and teaching needs. The Council moved to defer the Endorsement to the next sitting of the ISC.
6	**Annual Report:** ➢ Isaac S. provided an overview of the IS Annual Report. He noted that this will be presented to the GC Audit and the Planning & Budget Committees. He highlighted several accomplishments, including significant progress on MFA adoption and the continued year-over-year improvement in security maturity. It was also noted that there is increased participation of the DAI-IRSA program, which expanded the scope to include admin heads sign-off. ➢ Noted various Tri-Campus and divisional collaboration, including the log4j vulnerability Tri-Campus collaboration, which is an award-winning initiative. ➢ Ransomware remains a significant security risk. ➢ In terms of the future, will continue to take a risk-based approach through the strategic plan, new tool sets, unit-based risk program and the ISC. ➢ Need to ensure that investments are made and getting realized.
7	**University's response to recent concerns about mobile apps:** Kanupriya P provided the following overview, noting that the guideline on the use of mobile apps was done in consultation with the provost's office. She noted that the guideline is generic and not technology specific. It will cover all social media apps and will be released on the IS website. The plan is to keep monitoring for update and will follow the issue very closely and update guideline and standard accordingly. **Discussion Points:** ➢ The Council agreed with the university's response. ➢ It was also noted that other universities have taken our guideline and repurposed same. ➢ This is a good first step in taking a stance to better manage our mobile devices. The CISO's office will keep the ISC engaged going forward.
8	**Duo mobile app privacy** Raphael E updated on a request regarding information on MFA, DUO app privacy, specifically the

	type of information being shared with the third party and whether it is necessary or consistent with FIPPA? He presented a draft of the joint response (FIPPA/IS) for the Council’s feedback. **Discussion point:** ➢ Isaac S suggested extending an invitation to the requestor as a guest at an upcoming ISC meeting. ➢ It was confirmed that an information security and privacy impact assessment was done when acquiring this technology. The Council noted that the document was good to go.
10	**Any other business**: None
11	**Closing Remarks:** The Chair thanked members and guests for their time and commitment. There being no further business to come before the Council, the meeting was adjourned at 12:02 p.m. Minutes presented in the ordering of agenda, not in the order of the discussion.