Approved Minutes (PV)

Meeting:	**Information Security Council - Meeting**
Date & Time:	Monday, February 27, 2023 (10:00 am – 12:00 pm)
Location:	**VIRTUAL MEETING**

CHAIR:

Deepa Kundur

ATTENDEES:

Luke Barber, Rafael Eskenazi, Tero Karppi, Dimitris Keramidas, Alex Matos, Sian Meikle, Aidan Mitchell-Boudreau, Andrew Petersen, Zoran Piljevic; Rohith Sothilingam, Isaac Straley, Bo Wandschneider

BY INVITATION :

Sotira Chrisanthidis, Sue McGlashan, Paul Morrison, Deyves Fonseca, Carrie Schmidt, Kiren Handa

REGRETS:

David Lie

NOTE TAKER:

Andrea Eccleston

Item #	Item
1	**Welcome:** The meeting convened at 10:00 a.m. in with co-chair Deepa Kundur presiding. Co-Chair, Isaac Straley welcomed members and guests and introduced Co-Chair, Professor Deepa Kundur. He noted that this was the first meeting after an extended period and the delay was to ensure faculty participation for effective governance.
	Introductions: Co-Chair Isaac S asked members and guest to introduce themselves. This was followed by a round-table introduction.
2	**Approval of agenda:** The ISC agenda of February 27, 2023, was approved as presented. It was noted also that there is a lack of quorum.
3	**Approval of minutes:** The Chair invited comments from the Council regarding the Public and Full versions of the ISC minutes of Friday, March 25, 2022. The Public version of the ISC minutes was approved with the following amendment. Relevant to Item # 3 - **Data Asset Inventory & Information Risk Self-Assessment (DAI-IRSA) results -** need to include the details of the overview as referenced. **All in concurrence**
3	**Reflections on the past year and future priorities:** Isaac S provided an update on ongoing recruitment and retention initiatives. - Noted that the hiring process for a number of manager positions, new and existing, now finalized.

- Also updated that the Information Risk Program Coordinator position under the DAI-IRSA program has been transformed into a permanent seconded position. The plan is to fill this position from within the university on an 18–32 months cycle with candidates who have a connection to the divisions or academic space.
- Noted the ongoing use of contractors and casuals for staff augmentation.
- Also updated on a new initiative that would create opportunities for under-represented students with the goal of increasing diversity and inclusion.

In terms of other initiatives, noted the:
- Soft launch of the new branding of the IS website. Members can view @ https://security.utoronto.ca
- Also update on the status of the IS budget request, noting approval for an increase in the budget ask.

Isaac S also presented the following overview of key highlights, noting:
- The expansion of the university security protection via MFA.
- Ongoing work to increase the security awareness culture via individual and strategic initiatives.
- Ongoing collaborations, both internal and external:
- Working with the Temerty Faculty of Medicine on the active directory initiative.
- In term of national initiative, currently working with CANSSOC where a portion of the CISO time is allocated on this project. Noted that this project is currently receiving federal funding.
- UTORMFA enforcement for non-appointed staff and faculty completed with one major exception.
- MFA enrollment for student now sits at 92.6%, with the introduction of auto-enrollment on January 17th.
- The introduction of the next gen anti-virus, which is now available for everyone, including students.
- Also updated that a provider was selected for EndPoint solution following an RFP process.
- The IS Strategic Plan is currently underway. A draft version will be distributed to the members in advance of the next ISC meeting for evaluation and feedback. It was noted that a request for endorsement will also be made at the next ISC meeting.
- The DAI-IRSA report to be presented at the next ISC meeting.
- With respect to Vulnerability Management, the plan is to provide the Council with substantive data at the next meeting.

Action Items:
- To include "areas for future growth" regarding ongoing strategic planning initiatives as an agenda item for the next meeting.
- Kalyani K to share the draft Strategic Plan well in advance of the next ISC meeting material. Isaac S will be requesting the Council's feedback and endorsement on the plan.
- DAI-IRSA report to be a part of the agenda for the next ISC meeting.
- Isaac S to provide substantive data on Vulnerability Management at the next ISC meeting.

Reflections on the past year and future priorities:
Isaac S provided the following update in terms of the areas of priorities, noting that:
- Security awareness training is a top item.
- Presented data points on issues related to fraud prevention, noting that a Fraud Prevention Working Group is in place. A request made for the ISC guidance and input on the role of the Information Security team and the CISO in terms of the area of scope.

	- The Research Security portfolio now has a research information security lead through the VPRI. Also noted that there is a lot of national effort in this space. In terms of funding, will be brought back to the ISC for support. - The DAI-IRSA has received support for the unit head sign off process. - In terms of governance, noted plans to increase ISC engagement with the community as well as the frequency of the ISC meetings while being mindful not to overburden members' service obligation. **Discussion points:** A member asked if the ISC could endorse the recommendation for divisions and units in regards to investment in information security. The Council also held discussion about the need for a more coordinated approach in the academic units in terms of identifying the need to make investments in information security. It was noted that IS would provide support to putting more guidance in place, but cautioned on the need of having more structure.
4	**Privacy considerations for Microsoft Defender toolset and SentinelOne nextgen antivirus**: Isaac S noted that he would like the ISC to look at the impact of all our security programs. Information about steps taken to address privacy were presented to the ISC for consideration. A request was made for the ISC review, provide feedback, and support. **Discussion Points:** The Council provided the following feedback: - Noted that this speaks to most of the used cases and are reasonable. - Also discussed the issue of concerns about privacy and the need to make it accessible and transparent to the community. Will bring back to the table to discuss how to address in the most effective way. - Need to have plans in place on how to inform the community. **Action Item:** - Will bring back, Privacy considerations for Microsoft Defender toolset and SentinelOne nextgen antivirus, to the ISC table for discussion on how to address in the most effective way. -
5	**Section 889: Update, CISO Advisories:** Isaac S updated that this is a US requirement on certain use of technologies covering telecommunication equipment. He updated on ongoing governance and oversight efforts related to section 889 compliance, noting that: - This requirement also extends down to all contractors and UofT researchers who received US funding. - Noted that this issue has generated a lot of awareness and alignment at the P&D table. - The CISO, in partnership with procurement, has the accountability to drive enforcement. - Noted that Info Security will be moving forward to manage the global supply risk. In view of this, will be drafting security and privacy terms and conditions along with standards for the university when they go through the appropriate procurement channels. This would include defined RFP requirement that would restrict certain providers. Isaac S also reviewed the advisory process with the Council with respect to the process for issuing "warnings" and "cautions". **Discussion Points:**

	- The Council discuss the process for legal consultation. it was noted that this would be under the circumstances of an adversarial relationship with a country or company around sponsorship and other research activities. This would also include instance such as in the event there is a need to step outside of the boundaries of a template and make the language stronger. - Council also discussed the workflow and the need for greater assurance mechanisms. - Noted that there is an opportunity to pair this process by reminding people that there are approved vendors. - Plan is to be more strategic in this area where more curated list of options would be available. **Motion:** In lieu of this in writing, request submitted for the ISC endorsement to issue (might change the words) warning with this scope and caution until we review the option Andrew P brought up with the workflow. The key issue is that if we are going to issue a prohibition, need to bring forward to the ISC for endorsement along with other stakeholders. If this is a caution, we will move at whatever speed we need to, but consult as reasonable. **All in concurrence**
6	**Ransomware: Interim authorization for decision-making (discuss and endorse):** Isaas S updated on a number of concerning ransomware, in particular, Vice Society, which is actively targeting the academic space in North America. - Isaac S presented proposal that would enable informed decision-making in the event of a ransomware attack. A request for the ISC's endorsement to authorize the CISO, as an interim measures, to make decisions during ransomware attack was presented. **Discussion Points:** The Council held extensive discussion about: - The workflow. - University's preparedness to tackle such an incident. - The chain of command. - The consultation process. - The value of ensuring that the CISO's voice is in that conversation. - Decision-making process and the budgetary implications. - Suggestion made to tweak the wording of the proposal before it is put forward for endorsement. - The urgency of the issue and the need to have interim measures in place. **Motion:** In the event of a ransomware attack of any size, the CISO must be engaged. In consultation with key stakeholders (including Deans, Chairs, and impacted faculty) and the Tri-Campus Issues Management Group, the CISO is authorized to determine if ransom should be paid or not if consensus cannot be achieved. This is an interim decision and will be revisited in the April ISC meeting with additional consultation and a formal standard proposal. **All in concurrence** **Action Item:** - Ransomware: authorization for decision-making to be added to the agenda of the next ISC meeting.
7	**Update on website providing information on collection of student data** Kiren H. Executive Director, Institutional Research & Data Governance Office updated on the institutional data strategy, noting that there are a number of strategic goals to ensure

	transparency of data collected and its use. This includes:
	- Looking at how to modernize the way in which we communicate with students regarding how the data collected, used and protected for them.
	- Noted the link on ACORN to FIPPA provides a high-level articulation of that notice on principles and purposes.
	- This initiative was added to the strategic plan along with consultation with the FIPPA office and the Institution Research and Data office to look at how to communicate with students on the use of data.
	- Goal is to create a separate page to detail how students' information is collected, shared and protected in plain language.
	- Noted that an Advisory Group to provide oversight and a number of working groups were established to inform on the data flow.
	- An overview of the website which is still in production was presented.
	- Kiren H noted she would be happy to provide an update to the ISC at a future meeting.
	Discussion Points:
	- Aidan M-B thanked Ms. Handa for the work being done and inquired if there will be examples of how students' information is protected available on the webpage. In response, it was noted that this is not the full site and there are sections that provide more granular information.
10	**Any other business**: None
11	**Closing Remarks:** The Chair thanked members and guests for time and commitment. There being no further business to come before the Council, the meeting was adjourned at 12:01 p.m.