# Approved Minutes (PV)

**Meeting:** **Information Security Council - Meeting**

**Date & Time:** **Monday, January 31, 2022 (9:30-11:30 a.m.)**

**Location:** **VIRTUAL MEETING**

| **CHAIR:** |
|---|
| Heidi Bohaker |
| **ATTENDEES:** |
| Luke Barber, Eyal de Lara, Rafael Eskenazi, Tero Karppi, Dimitris Keramidas, David Lie, Sian Meikle, Aidan Mitchell-Boudreau, Andrew Petersen, Zoran Piljevic, Leslie Shade, Rohith Sothilingam, Isaac Straley, Bo Wandschneider |
| **BY INVITATION :** |
| Sotira Chrisanthidis, Jill Sue McGlashan, Paul Morrison, Deyves Fonseca, Carrie Schmidt, Deyves Fonseca, Robin Wilcoxen, Shannon Howes, Jill Kowalchuk |
| **REGRETS:** |
| |
| **NOTE TAKER:** |
| Andrea Eccleston |

| Item # | Item | Discussant | A | E | I |
|---|---|---|---|---|---|
| 1 | **Welcome:**<br>The meeting convened virtually at 9:30 a.m. with Heidi Bohaker presiding. The Chair welcomed members and guests and called the meeting to order.<br><br>The Chair updated the Council that a revised version of the draft letter to the Deans with respect to the Data Asset Inventory and Information Risk Self-Assessment (DAI-IRSA) was posted for members' review and feedback. | | | | |
| 2 | **Approval of agenda:**<br>The Chair invited comments from the Council regarding the meeting agenda. No changes were tabled.<br>**Motion:** To approve the agenda of the January 31, 2022, ISC meeting.<br>ANDREW P /SIAN M<br>**CARRIED** | | | | |
| 3 | **Approval of minutes:**<br>The Chair invited comments from the Council regarding the Public and Full versions of the ISC minutes.<br><br>**Motion**: To approve the Public and Full Minutes of April 28, 2021, ISC meeting as presented:<br>RAPHAEL E/LESLEY S<br>**CARRIED with no abstentions**<br>**Motion:** To approve the Public and Full minutes of December 10, 2021, ISC with the following amendment. Agenda Item 4, discussion points should read "Alex M to schedule meetings with Humanities and Social Science Chairs to understand some of the other issues that are non-STEM based".<br>LESLEY S/ZORAN P<br>**CARRIED with no abstentions** | | | | |

| | |
|---|---|
| 3 | **CISO updates:**<br>Isaac provided the following updates:<br>**ISEA Monthly dashboard:**<br>- Document was shared with the President's Tri-Campus Vice-Presidents Committee (TVP**)** and work is underway to create a version that can be shared at other senior tables such as the Principals and Deans (P&D) and Principals, Deans, Academic Directors and Chairs (PDAD&C) committees.<br>- He also reviewed the data points with respect to compromised accounts.<br><br>**Log4j vulnerability:**<br>- Updated on action taken, this includes ongoing investigation.<br><br>**November 2021 phishing incident**:<br>- Presented data points and updated on remediation measures being taken with respect to this incident.<br><br>**Multi-Factor Authentication (MFA)**:<br>- Noted that ISEA is making good progress but would like to move faster.<br>- In terms of the non-appointed staff, it was noted that the numbers remain quite low. With respect to appointed faculty, a significant amount of work was underway to get divisions to report by the deadline today.<br><br>**Endpoint Protection:**<br>- It was noted that work is currently underway to complete the RFP process to identify service providers.<br><br>**Security Awareness Training Pilot:**<br>- Noted that pilot is close to completion. In terms of the response from community members, a lot of feedback was received.<br><br>**Information Security Pause Week:**<br>Isaac S also provided an overview of the ISEA's Pause Week activities, noting that the goal was to pause, reflect and act on changes to achieve excellence in operations. He provided an overview of activities which include team-building exercises, professional development activities, designing anda pplying new processes and framework, and creating tools and artifacts..<br><br>**ACTION ITEM:**<br>- To add privacy discussion around Advanced Threat Protection to the agenda of the next ISC meeting.<br>- To add an update on the Security Awareness Training Pilot to the agenda of the next ISC meeting.<br><br>**Discussion Points**:<br>- The ISC raised the issue around the current international event and its potential impact on cyber security risk at the University. The council also discussed messaging and guidance for those faculty working in this area of research. Isaac S and Heidi B to take this discussion offline. |
| 4 | **MFA enrollment for faculty:**<br>Deyves F noted that there is the need for widespread adoption of the MFA as it is one of the most effective protections against security attack. He provided an overview of the various engagement models being used to socialize faculty members. It was also noted that this includes working closely |

| | |
|---|---|
| | with the Accessibility for Ontarians with Disabilities Act (**AODA**) Office and an AODA compliant webpage should be in place by end of February 2022.<br><br>In terms of support, it was noted that several solutions were implemented to address and mitigate faculty concerns. In terms of approach, the plan is to work with faculty through partnership with divisions to enable faculty to enroll by June 2022.<br><br>**Discussion Points:**<br>- It was confirmed that the faculty process for requesting hardware tokens is the same as the staff process.<br>- The ISC also discussed the process with respect to non-functional mobile devices. An update was provided on the service models available to resolve this issue.<br>- In terms of authentication issues with respect to Apple devices and the "remember me setting", a suggestion was made to update communication materials to include this information.<br>- A member also noted that there is a need to take important sessional dates into consideration such as, date of enrollment at end of term or beginning of the next term and the 10-day window after exam ends when final grades are due.<br>- The Chair encouraged faculty/librarian members to review the materials on SharePoint ahead of the next meeting as this item will be put forward for endorsement by the ISC at its next sitting.<br><br>**ACTION ITEM:**<br>- Deyves F to follow-up with the divisions regarding date and timing of exam window.<br>- MFA enrollment for faculty and librarians to be added to the agenda of the next meeting for endorsement. |
| 5 | **Data Asset Inventory & Information Risk Self-Assessment (DAI-IRSA) discussion and endorsement:**<br>Robin Wilcoxen, Information Risk Coordinator, provided an overview ofthe divisional level risk assessment program noting that:<br>- Data Asset Inventory & Information Risk Self-Assessment (DAI-IRSA) was officially launched in the fall of 2020 and originates from the Policy on Information Security and Protection of Digital Assets that was endorsed by the ISC in 2019. This policy states that each unit shall develop an Information Risk Management Program to be approved by the unit head.<br>- In 2020, in partnership with the Office of Institutional Research and Data Governance, a Data Asset Inventory component was added to help support the Data Governance Strategy for both units and the university.<br>- From a unit perspective, the DAI-IRSA provides a web-based toolset so units can systematically record their data assets and assess the information risk activities across 63 capabilities and identify gaps. Tableau reports are provided to help facilitate communication about risk posture and take action to improve.<br>- It was noted that for the current year, we are proposing to invoke formal approval process by asking Deans or equivalent Senior Administrators for major divisions to sign off on their DAI-IRSA to meet the Information Risk Management Programs policy requirement.<br>- A letter from the CISO, endorsed by the ISC, will be sent outlining the requirement of the policy to approve the Information Risk Management Program for their division. In terms of mechanism, this will be a single check-box submission from MS Forms link.<br><br>Robin W also reviewed the dashboard with the ISC. It was noted that divisions can benchmark their own efforts against targets that were developed during the external university risk assessment process in 2019 and benchmark their unit against the entire participation pool to provide some contextual information to help inform their decision.<br><br>**Discussion Points:** |

| | |
|---|---|
| | - It was clarified that for purpose of the program, divisions have the capability and flexibility in deciding how the approval process is managed within their sub-units. Divisions can have multiple assessments and they can make the decision whether heads of sub-units sign off.<br>- The council discussed the issue of flexibility to meet the timeline objectives and a suggestion was made to extend the date to March 15th. It was noted that the plan is to maintain the February 25, 2022, deadline.<br>- A member suggested the need to incorporate the DAI-IRSA sign-off into the annual accountability report sign-off process as info security impacts the entire community.<br>- Letter from CISO to Principals and Deans to be amended to include context with respect to when the divisional heads last received communication on the DAI-IRSA program. Letter should also include Robin Wilcoxen's title.<br><br>**Motion:** For endorsement of the letter from the CISO to the Principals and Deans informing about the program and the requirement of the policy to approve the Information Risk Management Program for their division.<br>CARRIED **with no abstention** |
| 6 | **Endorsement of the new Information Security budget proposal (reordered from item 7 to item 6)**<br>Isaac S provided an update on the IS budget. He reviewed the initiatives to be covered if the proposal is approved, noting that in terms of large spends, this would include End Point Protection, maintaining course on the MFA and funds for improvement to the systems and modernization process improvement.<br><br>**Motion t**o endorse the new information security budget proposal as presented.<br>**ROHIT S/RAPHAEL E**<br>CARRIED, Isaac S abstained |
| 7 | **Update on Fraud Prevention**<br>Shannon H, Director, High Risk, Community Safety and Crisis & Emergency Preparedness presented an overview of the fraud prevention program noting that over the course of the fall term the university has seen an increase in the number and type of fraud instances such as scholarship scams, gift cards. It was noted that lot of work was currently being done to stay current with these security threats. These include:<br>- The formation of a Fraud Prevention Working Group consisting of tri-campus representatives.<br>- Development of a multi-pronged strategy. This will be centered around education, general awareness campaign information, and ongoing work on statistical tracking and reporting method. Primary goal is to help all members of the community recognize what fraud scams look like<br>Members were invited to contact Shannon H or Kalyani K if they require additional information. |
| 8 | **Update on CanSSOC**<br>Jill Kowalchuk, Director, CanSSOC provided an overview, noting that CanSSOC started as a POC between 6 institutions, with Scott Mabury and Bo Wandschneider as the big drivers. In terms of the status, it was noted that the program is now in the pilot stage and has achieved several successes including funding from the government. In term of collaboration, have created partnerships with different institutions and global partners with respect to the delivery of threat intelligence via alerts. It was also noted that the program has a distributed team comprising employees of UofT/federated partners like ORION as well as other institutions. Jill also noted that the program is growing as the number of institutions is increasing.<br><br>**Discussion Points:** |

| | |
|---|---|
| | - How to balance collaboration with a clear commitment to the academic mission. It was noted that CanSSOC being independent from academic institutions can provide anonymity and provide an extra layer of protection that separates the institutions.<br>- Faculty input with respect to CanSSOC governance and the kinds of data sharing. It was noted that there is an opportunity to look at faculty inclusion in governance as part of CanSSOC's current evolution.<br>- Members were invited to forward their ideas and thoughts to Isaac S and Heidi B.<br><br>ACTION ITEM:<br>- To take the question of faculty/librarian engagement in CanSSOC governance structure offline. |
| 9 | **Any other business**:<br>None |
| 10 | **Closing Remarks:**<br>The Chair thanked members and guests for their time and commitment. She requested members to review the MFA rollout document as it will be up for endorsement by the ISC at the next meeting.<br><br>There being no further business to come before the Council, the meeting was adjourned at 11:40 a.m. |