Senate Committee on Information Technologies (SCIT)
October 12, 2020
Minutes of the Meeting

These minutes reflect discussion and debate at a meeting of a committee of the University of Minnesota Senate; none of the comments, conclusions or actions reported in these minutes reflect the views of, nor are they binding on, the senate, the administration or the Board of Regents.

[**In these minutes:** Call to Order and Introductions; Update on Canvas, Zoom, and Kaltura; Cybersecurity Initiatives and Data Security Policy; Discussion with Researchers Regarding Data Security Requirements]

PRESENT: Geoffrey Ghose (chair), Keith Brown, John Butler, Brent Christensen, Brian Dahlin, Santiago Fernandez-Gimenez, Bernard Gulachek, Kristin Janke, Pilar Karaca-Mandic, Lindsey Konerza, Kelvin Lim, Zachary Riffle, Robert Rubinyi, Daniela Sandler, Cassandra Scharber, Engin Sungar, Rielle Swanson, Matthew Weber

GUESTS: Mehmet Akcakaya

REGRETS: Whitney Taha Frakes

ABSENT: Yoichi Watanabe

OTHER: Brian Hanna, Naom Harel, John Strupp

1. Welcome and Introductions
Professor Geoffrey Ghose, chair, called the meeting to order and welcomed committee members and guests.

2. Canvas, Zoom, and Kaltura Update
Keith Brown, interim senior director for academic technologies, Office of Internet Technology (OIT), shared a PowerPoint presentation on current academic technologies, their use historically, and how use has changed since the onset of the COVID-19 pandemic.

- Use of Canvas, Zoom, and Kaltura has risen significantly since spring of 2020 when the University pivoted to online/remote teaching and learning.
- Metrics can be broken down for each of the system campuses and by individual colleges for the Duluth and Twin Cities campuses.
- Satisfaction rate for Zoom users from the University has been between 95 and 97%; some concerns around accessibility, Zoom responded by incorporating closed captioning and continues to improve accessibility.
- Requests for additions to Zoom features included:
    - Creating a version of "speaker view" for two or more people who may be copresenting but are in different locations.
    - The ability to prepopulate breakout rooms.

Brown then noted a few of the challenges that OIT has been working with:

- Technology is performing to expectations but there may be inconsistencies in how effectively end-users are implementing it.
- Varying start dates for classes across the system campuses made the implementation of multiple technology platforms difficult.
- Firewalls limiting student access are being deployed by other countries; international students may have some difficulty accessing class content.

Brown ended by saying that development offerings for both faculty and students around online teaching and learning were well attended this summer with 700 student participants and 437 faculty participants.

3. Cybersecurity Initiative and Data Security Policy
Next, Ghose introduced Brian Dahlin, chief information security officer, OIT. Dahlin briefly outlined the work and responsibilities of the University Information Security Services team and added that the goal of information security services is to always move toward preventative measures rather than reactive measures.

Dahlin then highlighted a number of current security initiatives in place at the University, including:

- Enterprise-wide HIPAA risk assessment to insure the University is in compliance with HIPAA security standards.
- General security policy updates.
- Improving the automation of security alerts.
- Shifting focus from the University's network to the hosts, servers, and systems that are associated with the network (for example, a significant portion of the University workforce is now working on personal devices rather than the University's network. Attention needs to be shifted to end-user devices to detect potential security risks and threats.)

Dahlin then noted some of the impacts of the pandemic and how it has increased the need for very intentional attention to security measures:

- Increased consultation around architecture security; as University personnel adapt to teaching and learning online, many new systems are brought into play to assist with the transition. Each of those new systems needs security consultation and assessment in order to be safely positioned within the University network.
- As the need for new vendors increases the need for comprehensive vendor reviews also increases.
- Identifying questionable vendors/practices and sharing that information with the University community.

Regarding policy work, Dahlin said he is not anticipating major changes to the following two policies which will be under review this year:

- Administrative Policy: *Data Security Classification*
- Administrative Policy: *Information Security Risk Management*

Dahlin then briefly described the five security policies at the University of Minnesota, all of which work together, he said, and can be found on the University of Minnesota Policy Website. The control levels that University members are expected to follow are based on the security classification of the information and are listed in the appendices of each policy.

Bob Rubinyi offered two suggestions related to academic technology:

- On the University's Learn Online website, provide specific *student-facing* information on data security since so many students are now accessing University resources remotely.
- Provide additional information *for faculty* regarding possible security concerns when introducing (to students) new applications or tools that may not be supported by the University.

4. Discussion with Researchers Regarding Data Security Requirements

Ghose next shared that, in regard to the policy language regarding controls for researchers, he had received calls from some colleagues about ambiguities in classification. He invited two researchers, SCIT committee member Kelvin Lim, and Mehmet Akcakaya, professor, Electrical and Computer Engineering, to share instances when they had difficulties interpreting the security policies.

Lim said that his human research data sets usually contain Magnetic Resonance Imaging (MRI) information and therefore a) are extremely large and b) must be protected and secured according to the Health Insurance Portability and Accountability Act (HIPAA) guidelines. He asked for clarification on how to approach the transfer of this type of material to remain in compliance with University policy. Lim noted that the National Institutes of Health (NIH) now requires, for many of its sponsored programs, public data release prior to publication, which may run counter to university policies about unpublished data.

Next, Akcakaya explained that in his area of work, he relies on public databases of human data to assist in creating and training algorithm programs. Even though the datasets are de identified, the University's policy requires that he classify the information as restricted (because it contains human data). That requirement, he said, along with frequently required server rebooting/updates, has the potential to severely disrupt research timelines.

Ghose then shared a link to the policy language in question (from Data Security Classifications By Type which is an appendix of Administrative Policy: *Data Security Classification*.) He asked Dahlin if a revision such as changing “human subject research data” to “data that contains personal health information” is possible and advisable. Dahlin said that the current language in the policy was developed in collaboration with people in the University’s research community four years ago and is what was recommended at that time. He added that, if adjustments to the policy language would help clarify what types of data fall into each category, those changes could certainly be considered during the current policy review period.

In the interest of time Ghose thanked the committee members and guests and adjourned the meeting.

Geanette Poole

University Senate Office