EXECUTIVE COMMITTEE MINUTES

Present: **Bearnes, Boudreau, Eklund, Kopocis, Krehbiel, Latta Konecky, Minter, Paul, Weissling**

Absent: **Baesu, Kolbe, Lott, Zuckerman**

Date: **Tuesday, December 13, 2022**

Location: **Nebraska Union, Big Ten Conference Room**

Note: These are not verbatim minutes. They are a summary of the discussions at the Executive Committee meeting as corrected by those participating.

1.0 Call *(Minter)*

Minter called the meeting to order at 2:44 p.m.

2.0 Announcements

2.1 Academic Calendar

Minter reported that the subcommittee looking at future academic calendars is still working but noted that the academic calendar has been set for the 2023-24 and 2024-25 academic years.

3.0 Approval of December 6, 2022 Minutes

Minter asked if there were any further revisions to the minutes. Hearing none she asked for a motion to approve the minutes. Eklund moved for approval which was seconded by Kopocis and then approved by the Executive Committee.

4.0 Faculty Concerns and Questions Regarding EM 16 (Vice President Blackman, CIO Tuttle, Deputy General Counsel Chambers

Minter noted that the Executive Committee asked for the meeting because of the continual concerns being raised about EM 16 by faculty members. She suggested that not all faculty members seem to understand that the changes to EM 16 is a response to the need for increased campus security and for insurance costs.

CIO Tuttle pointed out that whenever he has spoken with the faculty he has spoken about the importance and the reasons for revising EM 16, noting that cybersecurity is a major concern nationally for all enterprises. He stated that the information has also been shared in communications from his office. Minter noted that some of the communications discussed the changes in a philosophical manner rather than providing specific numbers on the cost of our cybersecurity insurance and suggested that sharing the actual figures might help people to understand that need for the changes to EM 16. CIO Tuttle stated that more of the deep detail figures could be shared and noted that cybersecurity insurance costs have gone up astronomically.

VP Blackman reported that he has had this discussion with the President's Council and with the Chief Academic Officers. He noted that in the past we had insurance coverage for $10 million dollars with a $25,000 deductible, but now we have $5 million dollar coverage with a $2,500,000 deductible. He pointed out that a lot of our peers have been dropped from cybersecurity insurance coverage and stated that crucial to not being dropped is to have tightened changes to computer policies, such as those made in EM 16, and required use of a duo authentication program.

Eklund noted that some federal grants are now requiring some level of insurance or high level of security at a university. VP Blackman stated that some of the granting agencies are placing a standard for required security and in many cases, universities are making the needed upgrade in security to meet those federal requirements.

4.1 What would be considered an "incident" that would trigger inspection of a faculty member's laptop or phone and who would authorize an investigation? Privacy and confidentiality are the main issues that faculty continually raise.

Minter stated that the use of the terms events and incidents is causing some confusion and concerns for faculty members, and she asked if these two terms can be defined. Deputy General Counsel Chambers stated that the less common occurrence is that someone might be misusing university IT systems, the more common situation has to do with public records requests or litigation where a court orders or the law requires the University to produce information. He noted when talking about personal laptops and phones it is a very, very rare occurrence and would predominantly come up with a public records request or litigation and only when an employee is using a personal device to conduct university business. He reported that if this were to occur someone from the General Counsel office calls the employee and asks if they have information on personal devices pertaining to the public records request and in most cases, it would be something in an email. He pointed out it is usually a very collaborative process with the employee only needing to send a copy of the business email or text on their personal device that is being referenced in the request. He noted that he cannot think of a time when the General Counsel office has taken physical custody of someone's personal device.

Latta Konecky asked what would make her personal device vulnerable to one of the mandates. She pointed out that she uses her laptop for duo authentication and asked if using it makes her personal device more vulnerable. VP Blackman reported that the FAQ has recently been updated to address concerns from the campuses and the document can answer many of these kinds of questions, but basically a faculty member can download their course shell on their personal device with no problem. He pointed out that where EM 16 comes into play is if someone is storing medium to high-risk data on their personal device. He stated that in cases of an email message, these are stored in the cloud, not on the personal device. He reported that any public records request must first go to the General Counsel office for review.

Weissling asked if an instructor is downloading grades from Canvas on a personal laptop, without student social security numbers, would this be considered medium-risk data. CIO Tuttle stated that an instructor can download the grades, but they should be deleted afterwards from your personal device. He pointed out that if an instructor wants to retain the information, they should store it in OneDrive. He reported that an ITS team is working on developing some supporting materials to help instructors with downloading the information from their personal device to OneDrive. VP Blackman stated ITS gets a lot of inquiries about what is considered medium and high-risk data but noted that there are different kinds of data such as research, student, and faculty data but ITS does not define data definitions. He stated that the Office of the Registrar and the Office of Research and Economic Development make the decision regarding what is considered medium and high-risk research data.

Minter reported that there are some faculty members who have been targeted by outside political interests and it is unclear to them whether the new EM 16 takes away some of the protection they previously had in terms of privacy and that it opens employees up to a higher level of surveillance in their professional life. Deputy General Counsel Chambers stated that no one from the General Counsel office is conducting surveillance on an employee's personal device or university computer. He pointed out that if a public employee is texting about work on their phone and a public record request is received, an employee can be required to produce the texts relating to work. However, he stated that the majority of the time General Counsel wants to collaborate with the employee in fulfilling public records requests and does not want the employee to have to go through the lengthy public record process.

Latta Konecky suggested creating a best practices document explaining what kinds of work employees can conduct on their personal devices which would more than likely not be subject to a public records request. She also suggested having a preamble explaining that there would need to be an extraordinary incident for your personal device to be investigated.

VP Blackman pointed out that EM 16 had not been updated since 2001 and while the revisions to the policy articulate the university's position on some of the questions being raised, the revisions have not changed the university's practice. Deputy General Counsel Chambers agreed and affirmed that the changes to EM 16 are not going to change the practices of the university and General Counsel.

4.2 EM 16 states that the university "retains the right to review files, email, and data for compliance with policy and its business purposes." How would the university ensure that confidential and sensitive data, including data bound by ethical and legal commitments, be protected from surveillance if a review is conducted on a faculty member's computer?

Minter noted that IRB approval requires that data collected through research must be kept confidential and she asked how faculty can be assured that this data would be protected if a review of a faculty member's computer is conducted. Deputy General Counsel Chambers pointed out that most of the data that would be collected would be housed by the university and the researcher is an employee of the university so he does not believe it would be a breach for the university to internally make sure that the data is secure. He stated that only specific people working for the university could review the data and these employees are required to keep any information confidential. CIO Tuttle reported that

ITS employees must sign a confidentiality statement each year during their annual evaluation, and they are fully aware that part of their job is to maintain confidentiality.

Latta Konecky asked if any of the questions in the FAQ address the IRB requirements. CIO Tuttle stated that he would need to check this out, but it could be included in there. Latta Konecky pointed out that sometimes the questions being asked by the faculty are not clearly addressed in a response because there is a difference between the layman's term used by the faculty and the IT technical term. She suggested that using the same language could help ease some confusion. VP Blackman stated that he appreciates this suggestion and noted that ITS wants to make the FAQ as clear as possible for everyone.

Minter reported that some faculty members wonder how a policy such as EM 16 could be developed without some faculty input. She asked if there was any faculty input when the revisions were made. CIO Tuttle stated that when the process was started to review EM 16 it was discovered that the policy was 20 years old. He reported that the feedback from the campus and university-wide leadership was to work with those who deal with high-risk data and not to have the faculty perspective early in the process because this was a matter of IT security. He pointed out that a summary of proposed changes was presented to the Faculty Senate's Information and Technologies Services Committee and presented at a spring Faculty Senate meeting and the policy was signed and put into place shortly after that meeting. Minter stated that although the revised policy was included in the spring Senate packet, it was a surprise to faculty members who are not members of the Senate.

4.3 Will faculty who use their personal laptop to conduct university work be required to have the endpoint management system installed on their personal laptop or phone?

CIO Tuttle stated that the endpoint management system needs to be installed only on new, university owned computers, not on a personal computer. However, ITS does recommend that you have Cortex or some other security program on your personal computer.

VP Blackman stated that an end-point management system is a tool that allows the university to get the latest updates quickly on computers to protect university owned devices. He pointed out that to manually go around to either talk people through installing an update or manually installing it on each computer would be impossible.

Eklund stated that comments he has heard is that if people are doing other work on their time off from the university that is their business, but they wonder if their research or creative work belongs to the university. Deputy General Counsel Chambers pointed out that the university has a conflict-of-interest policy. He stated that the university does not look at someone's email or cloud protected documents to see what work is being done. Eklund noted that copyrighting and intellectual property rights are a huge issue that can generate a lot of money. Deputy General Counsel Chambers pointed out that the university has NuTech Ventures which protects and licenses the university' intellectual property and promotes entrepreneurship.

Deputy General Counsel Chambers reported that there is training available about public record requests, and he would be happy to arrange for the Faculty Senate to have a training session if there were people interested. Minter stated that the Executive Committee will consider this and thanked VP Blackman, Deputy General Counsel Chambers, and CIO Tuttle for their time and willingness to speak to the Executive Committee.

4.4 Some faculty in the Physics Department are reporting that Cortex conflicts with some of the software they have to use. What is the plan for faculty where that is/may be the case?

CIO Tuttle reported that there are some cases where faculty are unable to put Cortex on their machine or that it causes problems. He stated that 99% of the time ITS can get the program to work correctly and he reported that ITS works with faculty members to try to resolve the issue.

Kopocis noted that the university has an enterprise edition of Cortex and one for personal use. She asked what the difference is and if using Cortex on your personal computer opens your personal data to the university. CIO Tuttle stated that having Cortex on your personal computer does not enable the university to look at your personal data. Kopocis asked if there is any live monitoring with Cortex. CIO Tuttle stated that there is not, and VP Blackman pointed out that the university does not remote into a person's computer through Cortex. He pointed out that there is remote tech support where an IT person can remotely access your computer, but you must first authorize it and it is recorded.

5.0 Unfinished Business

5.1 Update on ITSC's Recommendations on Faculty Senate's Policy on Acceptable Use of Software Systems Management & Deployment Tools

Minter reported that Professor Leiter is stepping in as chair again of the ITSC and she has been in communication with Leiter and CIO Tuttle about the Senate's policy now being in conflict with EM 16, but she does not have any updates to report at this time.

5.0 New Business

No new business was discussed.

The meeting was adjourned at 4:22 p.m. The next meeting of the Executive Committee will be on Tuesday, January 24, 2023, at 2:30 pm. The meeting will be held in 201 Canfield Administration Building. The minutes are respectfully submitted by Karen Griffin, Coordinator and Signe Boudreau, Secretary.