ACEC Final Report FY2019

Meetings:

Sept 21, 2018

Nov 13, 2018

Feb 14, 2019

March 7, 2019

Meeting notes are available in OneNote Online at:
https://kansas.sharepoint.com/teams/governance/ACEC/_layouts/15/WopiFrame.aspx?sourcedoc={7cdc743f-155b-4cdc-b51e-5565be1ba7ad}&action=edit&wd=target%28MeetingNotesFY2019.one%7Cfc629f7b-37cd-4939-a307-6e6d59fd0d2e%2F%29&wdorigin=717

Specific Charges

Continue to review Blackboard from the perspective of functionality and cost, including cloud hosting mode and the mobile version of Blackboard.

The committee discussed the use of Blackboard and alternatives in more than one meeting. None of the committee members have mentioned experiencing serious problems with Blackboard. Several mentioned positive experiences, such as with flipped courses. The recent activation of Blackboard Observer for the KU Athletics is also relevant. We invited Mary Walsh (KU CIO) to describe her experiences at Tulane, which did switch from Blackboard to Canvas.

Mary noted that, in contrast to KU, at Tulane there was considerable dissatisfaction with Blackboard. This contrast might be due to changes in Blackboard or to better support at KU. At Tulane mixed classes (undergraduate and graduate) were a challenge with Blackboard.

Tulane did a pilot study to try out alternatives (Desire2Learn, Canvas, and Blackboard). Canvas was the hands-down winner. In the resulting transition to Canvas, volunteers switched first. Following the transition usage of Canvas increased over the previous use of Blackboard.

Mary noted that Canvas would likely be significantly more expensive than Blackboard, perhaps twice as much. We would also need a transition period in which both products would need to be licensed. Transition would entail other (labor) costs to convert course materials to a new system.

Conclusion

Given the substantial costs in switching we are not recommending pursuing any immediate transition to an alternative to Blackboard. One approach might be to renew Blackboard for two to three years and then reevaluate.

Follow-up and review any new IT policies received by SenEx, proposed by IT.

The new policy on multi-factor authentication is discussed below.

Continue to monitor IT efforts to determine varying needs of multiple user communities on campus, and recommend possible improvements. Evaluate the effect of process changes to Faculty, Staff and Students shared mailboxes.

The committee is pleased with the openness of the new KU CIO, Mary Walsh. She, for example, has volunteered to attend the ACEC meetings. A committee member also suggested that it would be useful for her to attend some department faculty meetings, in the humanities as well as in the sciences.

Committee members mentioned a few specific IT needs on campus.

- There can be challenges to conducting remote control of experiments across the campus network. These include firewall issues and older equipment controllers that can't be networked.
- One member mentioned that it is increasingly difficult to use grant money to purchase computing equipment.
- Purchasing rules need to account for unique needs of research equipment. "One size fits all" contracted equipment is often inadequate. This needs to be counterbalanced against efficiency of equipment support. Commonality across equipment allows for better use of spare parts and support staff knowledge.
- Over-reliance on the software aggregator (SHI) creates problems for purchases of software available from a single vendor. In these cases, there have been continuing problems with renewals of annual licenses or in payments to the actual software vendor.
- Storage is a big issue, increasingly across domains, for both working storage and archival storage.
    - As an example of working storage needs, one committee member in the arts will need to store up to 100TB per year of video. These also need to be used across multiple years.
    - KU also has no cross-university approach to long term archiving of research data. We have ScholarWorks, but that is not designed to curate data as data with the ability to search by data-specific metadata (like variables or measurement types). This ability is important for reuse of data. Some domains do have access to domain-specific archival storage through KU membership in consortia. An example is ICPSR for the social sciences. Funding agencies commonly require some sort of public access to generated research data. This will become a compliance issue for KU.

As to the changes to shared mailboxes, one staff member has mentioned that the renewal notifications are somewhat heavy-handed, coming as an annual message to each individual account threatening to shut off the account if there was no response. Another staff member mentioned that sending mail-merge email by proxy requires an administrative account work-around. This formerly was possible from a user account via proxy.

Investigate best practices in training and providing the proper tools across campus to increase use of software.

We noted the adoption of Lynda.com access http://humanresources.ku.edu/lyndacom-0, via Linked in Learning. This is a one year agreement with renewal dependent on usage. There have been a couple of campus wide emails pointing out this service.
We also understand that there is an administrative group looking at enhancing the University's training. One committee member asked if in-person training could be added to the My Talent professional development record.

Meet with the IT Security Officer to establish protocols to ensure maintenance of individual privacy in technology implementation

The committee met with Julie Fugett, Chief Information Security Officer to discuss maintenance of privacy. Julie stated that the IT Security Office (ITSO) must be concerned with security first and privacy second. She then gave the example of the ITSO vendor questionnaire and its questions about data protection as an example of privacy protection:

- Is KU's single sign on possible or must there be a vendor account?
- How is data protected?
- What happens to data once KU is no longer a customer?
- What is encrypted?

- Who at the vendor has access to the data?
- What is vendor training?
- Can vendor staff download KU data?

She pointed out that IT policies go through several levels of review, including the General Counsel's office and the CIO. Another example Julie mentioned is that the Duo system (see below) will be set to not allow users to opt-in to sending performance data to Duo.

Our conversation then turned to the recent, new Multi-Factor Authentication (MFA) policy. While the shift to MFA has already been announced as being in force as of October 1, 2019, the policy itself is apparently still in the works. Faculty, staff, and (employed) graduate students will be required to use a secondary device to authenticate when signing on to any of the KU systems behind single sign-on as well as when using the KUAnywhere VPN. Undergraduates, and those who have left the University will not be required to do secondary sign-on. Departments may opt to include their student-hourlies. IT will work with departments wanting to put other systems behind the MFA system.
The preferred option will be to use the Duo app on a smart phone or tablet. Other alternatives are typing in a passcode from a text message to a mobile phone or the use of a Universal 2nd Factor (U2F) security key. The latter technology appears to have some issues. The key can get out of synch with the Duo system necessitating a reset. The U2F keys are an option for staff who do not have access to a mobile phone and could be purchased by their department. Julie anticipates a purchase price of about $10. Central IT may purchase some tokens to be distributed to departments as well. Some universities sell the security keys through their technology shop. There will also be an option for the IT Customer Service Center to generate an emergency key to allow login by someone who has temporarily lost access to their phone. This center is open about 37 hours per week.
There is a setting allowing a particular browser (e.g. Chrome) on a particular machine to be set to remember the secondary authentication for 30 days. This should make the transition easier for staff who are required to log in to multiple university systems many times a day. The app is also ADA accessible on many devices. Individuals wanting to make the transition before their department is scheduled may enroll at: https://myidentity.ku.edu/multifactor.

This policy has been prompted by several successful hacking or phishing attacks against KU people, including one attack involving personal financial settings and another involving grades.

Conclusion

Committee members felt that this policy will improve the security of access to campus systems. It will, however, need to be implemented with serious attention to potential impact on staff or students for whom access to an appropriate device is difficult for financial or other reasons.

Follow up on town-halls focused on IT policies and issues

Mary Walsh would be happy to have IT related town halls. The committee feels that the scheduling should be done by KU IT.