FY2018 Academic Computing and Electronic Communications (ACEC) Final Report

The committee met three times: October 4, 2017; December 5, 2017; and March 13. Again this year we kept minutes in OneNote in the ACEC committee SharePoint (MyCommunity) site.

Charges for 2018 were:

"Standing charges:

1. *Monitor current and proposed policy concerning security of information, intellectual property rights and responsibilities, and other matters relating to information technology. Identify issues for which policy should be developed or revised. Report issues and any recommendations for action to SenEx. (ongoing)*

Specific charges:

1. *Look at the various options for exploring alternatives to Blackboard from the perspective of functionality and cost.*

2. *Follow-up and review the new IT policies, proposed by IT. (Info Tech Security Policy, Server Registration Centralization, Security Incident Response Policy, Data Classification and Handing Policy.)*

3. *Continue monitoring collaboration tool rollout–Office 365, Skype for Business including Voice Over IP (Skype for Business phone service), etc.– and obtain or produce a cost-benefit analysis of each. Work with KU IT on ways to integrate third-party software (e.g., Dropbox, Google Docs) into its collaboration tool portfolio.*

4. *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.*

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

"

Specific Charge 1

We discussed Blackboard several times. While a number of universities have switched to alternatives the sense of the committee is that there is currently no pressing need to seriously pursue alternatives. A great deal of effort has gone into KU faculty course design using Blackboard and any transition must consider the cost in people time to make a change. One motivating factor for change might be if Blackboard moves to a cloud hosting mode that forced major changes in current KU materials or compromised the security of FERPA protected information.

Alternatives that other universities have adopted include Moodle, Sakai, and Canvas.

Specific Charge 2 (IT policies)

The committee met with Julie Fugett, Chief Information Security Officer to discuss these policies. Our first discussion centered on how these policies interrelate. The Information Technology Security Policy drives the other policies. Other policies are spawned when a topic includes too many details to include in a single policy.

We also asked how these policies are developed. Some policies are developed in response to regulations from outside the University, e.g. state and federal regulations. There is a long sequence of review for these security related policies. The Information Technology Security Office (ITSO) develops an initial draft which then is passed through a number of other bodies, including the Policy Office, Deans and Directors, General Council, Governance committees and Governance leadership, a vice Provost, and the Provost.

This led to a question about how these policies and changes in the policies were communicated to the University community. How is input from the broader community solicited during development of the policies? Administrative bodies may not always be aware of specific implications of the policies. One suggestion was that there should be periodic "town-halls" for IT related issues, much like the parking town halls.

We asked to what degree is KU constrained by Kansas Information Technology Executive (KITEC) policies. KU can request waivers from these policies where necessary. The password policy is an example. KITEC password policies (e.g. account lockout after 5 failed entries) would not be workable on campus.

This discussion raised the question of whether the current KU password policy should be reviewed (see recommendations below).

One comment was that many elements of these policies just codify what is being done already. Another general comment was that hyperlinks to definitions of terms in the policies would be helpful.

We had an additional discussion about the consequences sections of each of these policies. One committee member asked how those in the University community could know what constitutes a violation of the policies. The Acceptable Use and Email polices contain examples of non-acceptable behaviors as does the online security training in My Talent. Specific questions could also go to ITSO.

The Policies

Information Technology Security Policy

The discussion on the Information Technology Security Policy focused mainly on how the existence of security training is promoted. Campus-wide emails and notifications in the Talent Development System seem to be the primary mechanisms. People who respond to the self-phishing exercises are also encouraged to take security training.

Server Hosting Policy

This policy came about as an update of a server centralization project which ended before completion. It is intended to meet an ongoing need for servers for new functions. This is a critical need in the research sector where there may not be an existing server that can perform the needed function.

Ms. Fugett pointed out that a poorly supported server poses multiple risks. It might expose sensitive data. It might serve as an attack vector inside of KU's network security perimeter, leading to other compromised systems. The biggest concern is a poorly managed server containing highly sensitive (Level 1) data. Servers not containing sensitive data may be missing security safeguards that make them a threat to other systems on campus. This is true for other computers as well, but servers, by design, may be more exposed to hacking than ordinary workstations (e.g. via open ports for their services). One example she mentioned was a case where fraudulent unemployment claims were made on multiple KU staff members after data were compromised.

This policy needs to be implemented in a way that provides as few barriers to cooperation as possible. We noted that people will find ways to get their work done. If a central service does not meet that need and a quick alternative exists, then the central service may not be chosen.

The committee also asked about "Cloud" services like Amazon Web Services (AWS). There is a contract in place through Internet2 via and AWS reseller for such cloud services. A KU user must be arranged through Procurement Services. There is no current contract for Microsoft Azure or Google Cloud services.

For storage services, Dropbox for Business has been approved for some uses (including HIPAA level data). In one research project a researcher was able to use Dropbox for Business to manage secure data in an international location where the KU VPN was inaccessible. This required a contract with Dropbox needing approval by ITSO. Note that this is **not** Dropbox basic, which is not approved for secure data.

The committee asked how these arrangements with external vendors work in terms of ownership of data, management of the data after the contract ends, access control, security procedures, server maintenance and so forth. A contract with the vendor must address all of these issues.

Implementation Barriers

Cost was mentioned as one barrier. If setting up an independent server is much cheaper, the temptation is great. Cost, in this sense, is not limited to financial cost. If central servers are too limited in functionality, or if their setup is too burdened by administrative paperwork, the central solution may not meet needs. This is particularly true in the research sector, where timelines can be tight.

This policy has serious implications for the research sector. **Central IT's model of "create a ticket for that" does not meet the need of research projects to set up servers with non-typical configurations.** Its staff seem unwilling to cooperate in addressing security issues outside of their comfort zone. It is difficult to find someone in IT to even talk to about server setup. Different technical people may have different sets of skills and teamwork is often needed in novel situations. Calling 864-8080 is not teamwork. IT also needs to be much more responsive and flexible in providing information in advance of server setup. A grant proposal will need cost estimates for potential servers and faculty developing grants will need consulting on configuration of centralized servers. Timelines in these cases are also tight. Staff members have reported that the process for getting information about potential virtual servers could be improved.

Ms. Fugett also noted that there will be exceptions to centralization under the policy. Some laboratory equipment, for example, may need a direct high speed connection to a server.

Security Incident Response Policy

This policy describes the manner in which suspected information technology security incidents should be reported and the organization of the response within KU Information Technology (KUIT).

This needed to be a separate policy both for KU's internal needs and to comply with external mandates (e.g. HIPAA, and Kansas Information Technology Executive Council policies). This policy also depends heavily on the Data Classification Policy.

Data Classification and Handing Policy

We noted that this policy has evolved over time to define the categories in terms of degree of risk, rather than via specific data attributes. Specific examples are now included in a "quick reference" appendix. There is also a Quick reference listing the categories for some specific types of data (e.g. HIPAA, audit reports, course offerings).

Specific suggestions

Some of the items in this appendix may be overly general or may belong in some other more detailed policy.

Section 4E of the appendix, for example states: "E. Refer requests for information from media representatives (i.e., reporters, TV news crews, etc.) to the Office of University Relations.". More than a few research projects produce data for public consumption through web applications. Is the Office of University Relations really going to review all of these data?

Section 5C is about faxes but refers to emails.

Recommendations for Policies

A policy like the Server Hosting Policy has implications for resources and staffing for KUIT. If the policy is to be successful KUIT will need to take on more of a facilitator role and not be merely a utility.

The KU password policy should be reviewed in line with recent revised recommendations from the National Institute of Standards and Technology (NIST - https://pages.nist.gov/800-63-3/sp800-63b.html#appA). Some of the recommendations might make life easier for faculty and students, for example focusing on length of password over complexity and using blacklists to disallow known bad passwords. Locally overused passwords could also be disallowed by looking at frequencies of the password hashes. Dual factor authentication, for example, would be preferable for accessing sensitive data.

IT should consider holding periodic town-halls focused on IT policies and issues.

Specific Charge 3 (tool rollout, and third party software)

The committee felt that this is a topic that needs broad community input.

As to integrating third-party software into the portfolio of tools available to the KU community, we did note that ITSO has approved the use of Dropbox for Business (not Dropbox Basic) for sensitive data as mentioned above. This, in fact, may be one of the only options for collection of sensitive data in international settings where encryption and KUAnywhere are not available. An important factor is the ability to have a contractual arrangement with the vendor that specifies how the data will be handled in alignment with KU data security policies.

Specific Charge 4 (user community needs)

Many of these issues deal with KU community opinions. We noted that there could be better mechanisms for revealing these opinions than through the experiences of a few committee or administration members. One alternative would be yet another poll. Another suggestion was for IT to host periodic town hall meetings as does KU Parking. These meetings could be moderated by ACEC.

Committee members suggested that IT could make proposals to the community in such a forum prior to final decisions to roll out replacements for existing facilities.

Specific Charge 5 (training and software use)

The committee has invited KU IT a trainer (Suzie Johannes) to make several presentations in the last two years and has been impressed with the quality of her instruction.

We discussed the use of online training at other universities as well as the use by some KU departments.

Some Universities have contracts with online providers like Lynda, Udemy, or PluralSight that allow students and staff to take online training classes for free. We noted that Lawrence Public Library currently offers access to Lynda.

In terms of the use of software we did also note that KU’s funding mechanism (user fees) for campus-wide licenses sometimes serves to restrict rather than encourage use of tools we pay for.