University Senate Academic Policy and Procedure Committee
Report on KU IT Security
March 15, 2018

The following document provides a report on Specific Charge 3: *Working with the IT Security Officer, AP&P should establish protocols to ensure maintenance of individual privacy in any changes to technology implementation.* It was prepared by AP&P Chair Karen Moeller with assistance from committee members Lea Currie, Monica Simonsen, Nancy Jo Kepple, Mohamed El-Hodiri, Joo Ok Kim, Joe Walden, Martin Nedbal, Matt Deakyne, Furqan Mohammed (Vice Chair), Sarah Jean Coughlan, Jason O'Connor (ex-Officio) and Karen Ledom (ex officio).

Members of the AP&P committee met with Julie Fugett (Chief Information Security Officer) and Mike Rounds (Senior Associate Vice Provost for University Administration) on November 9, 2017 (see minutes dated 11/9/17) to discuss Charge 3.

The meeting addressed the following three areas in regards to Charge 3: Software Management, Change Management and Security Management.

Ms. Fugett first discussed the Change Management Process how individual privacy is protected when changes to technology are implemented. She explained how KU IT must adhere to many regulatory requirements (e.g., FERPA, HIPPA, and Controlled Unclassified Information (CUI)) that also encompasses privacy concerns and are very stringent concerning personal data. When making changes, upgrades, or providing sensitive information/data, privacy and the effects across campus are a top concern of KU IT and is always considered prior to change. Mr. Rounds discussed how IT is currently strengthening their Change Management process. KU IT is presently working on a governance model for change management to be transparent and to include the correct stakeholders when considering changes. Currently, the Academic Systems Steering Committee fulfills this role in regards to Blackboard and other Educational Technology tools. More information on this committee can be found here: https://blackboard.ku.edu/steering-committee.

In evaluating Software Management, it was discussed that most software licenses are specific to KU or KUMC but at times licenses are shared between campuses. Mr. Rounds discussed that KUMC has a mirror IT organization with their own policies and procedures. KU IT collaborates extensively with KUMC IT when appropriate but each organization has different processes and policies which can create some challenges in transparency. John Godfrey is KUMC's Chief Information Security Officer.

With respect to support management for software/applications, all KU IT employees who manage applications (e.g., Blackboard) that contain FERPA or HIPPA data must take the necessary training. Additionally, KU IT restricts access to applications for support purposes only and is limited based on the employee's position. All interactions with systems are logged, and changes are tracked, specifically to document any abuse of access.

One concern the AP&P Committee expressed was faculty using software/applications not purchased by the University but purchased by the faculty themselves and not vetted by KU IT. Although KU IT does not want to restrict faulty from using outside software, the faculty member is taking the risk of using a non-vetted program. Ms. Fugett expressed that she tries to make herself as visible as possible to the KU community and is open to meeting with faculty/staff/departments early on in evaluating an application/tool to help departments/individual's assess security concerns or guide them to use a supported application.

Lastly, security management was reviewed. Ms. Fugett and Mr. Rounds expressed that security is one of KU IT's top priorities and Mr. Rounds expressed how they are strengthening and adding additional resources to information security.

A concern from the AP&P committee was information security of lecture hall computers (e.g., universal logins, open access to install external programs) and the recent discovery of "keystroke loggers" being found on campus. To protect security in lecture halls, Ms. Fugett had the following recommendations for users of lecture hall computers:

- Connect laptops to classroom monitors and avoid the use of lecture hall computer.
- Inspect classroom computers for keystroke loggers before use (e.g., look for any devices between the keyboard and the computer)
- Avoid logging into programs on the classroom computers (e.g., email, blackboard)
- Bring lecture material on external device (e.g., thumb-drive) to avoid logging into external applications (e.g., Dropbox, email)

KU IT is currently in the process of exploring multi-factor authentication to make logins more secure.

The AP&P committee appreciated meeting with Ms. Fugett and Mr. Rounds and felt that appropriate procedures are in place to ensure individual privacy in any changes to technology implementation. They addressed all the committee's concerns and are currently strengthening their security and change management processes. Based on the meeting the AP&P committee recommends the following:

- Implement multi-factor authentication for increased security in addition to using single-sign-on for all KU supported applications.
- Increase awareness across campus of security issues by attending faculty/staff meeting and including security tips in their email newsletters.
- Re-evaluate the security of lecture hall computers.
- Remind faculty/staff of the Acceptable Use of Educational Technologies policy when using non-KU supported programs.
- Encourage faculty/staff to share recommended programs with the Academic Systems Steering Committee.
- Enforce annual security training (e.g., FERPA, HIPPA) for all employees (faculty/staff) with access to sensitive data.
- Schedule yearly meetings between CISO and the AP&P committee to address concerns.