Technology Committee Year-End
Report of Activities, 2017-2018

Members:
• **Chair**: Cameron McLeman (CAS)
• DeAndre Shepard (SEHS)
• Suleyman Uludag (At Large)
• Lyn Behnke (SON)
• Keith Moreland (SOM)
• Leslie Smith (SHPS)
• Huda Sheikh-Khalil, Student Representative
• Anushika Srivastava, Student Representative
• Scott Arnst (Director, ITS), *ex officio*
• Harvey Sherman (Associate Director, ITS), *ex officio*

Agenda Items:

1. The committee routinely approved some requests to send messages to the UMF-FAC_Staff email list.
2. The committee fielded some questions/concerns from faculty through Faculty Council about the use/placement/necessity of Smartcarts in classrooms. After deliberation, the consensus was to solicit faculty input via survey.
3. The committee decided not to draft its own survey, but rather piggyback on the infrastructure of an annual survey deployed (and at the time, being redeveloped) by ITS. The committee drafted some recommendations to ITS for questions to be included in the survey. As of late April 2018, ITS says the survey should be deployed “very soon.”
4. The committee approved the creation of a “Campus Emergency” email group for timely dissemination of emergency communications.
5. The committee fielded a request from ITS to consider the possibility of using student employees for the purpose of resetting faculty and staff passwords. Being the most contentious discussion of the year, I am including a summary of the discussion, in the form of the email sent to Faculty Council by the committee, on the next page. Both faculty council and this committee unanimously approved the change to allow well-vetted student employees this role.
Greetings Dr. Alfaro and Faculty Council:

I am writing on behalf of the Technology Committee in response to a proposal we are considering, involving the use of student employees to reset faculty and staff passwords. There was some internal debate about the protocol and we thought it best to err on the side of caution and bring the matter to the council.

If you'll bear with me, I'll walk through the current protocol for password resets before explaining the proposed modification. Currently, if someone wants to reset their password, they can first attempt to do so automatically using the self-service password reset functionality here:

https://password.umflint.edu/pwm/public/ForgottenPassword?

(The site will ask them some security questions and then guide them through the automated process).

Alternatively, they can call the helpdesk directly to achieve the same goal (the helpdesk will typically attempt to direct them to the above link as well). If the caller can't or does not want to use the automated reset, the helpdesk employee can manually reset the password and verbally relay a temporary password to the caller, who will then be forced to choose a new password the next time they log on.

Currently, only full-time employees at the helpdesk have the authority to do this manual password reset, and so student helpdesk employees currently have to track down a full-time employee to take care of such a caller. The proposal before us is to give select student employees this authority as well.

Potentially relevant factors, synthesized from the internal conversations our committee has had on this proposal and from conversations with Scott Arnst (Director of ITS, who supports this proposal):

1) Without needing to spell them all out, I think it's safe to say that the more or less obvious worries/objections fall into the general category of the potential for misuse of this authority by student employees.
2) The use of students for such a purpose is currently the protocol in place at Ann Arbor.
3) A principal goal of the proposal is to reduce costs and improve morale-- in particular, currently we pay overtime to full-time employees to work Saturdays so that someone is around with the authority to reset passwords.
4) Only experienced students deemed sufficiently trustworthy would be given this authority. Improper use of the authority would be a fireable offense (a significant consequence for students looking to enter into ITS as a profession).
5) All password resets are logged, and would be traceable to the helpdesk account that triggered the reset.

I hope that I have included and accurately synthesized all of the relevant details. I invite any questions you might have for the committee.

Regards,

Cam McLeman, on behalf of the Technology Committee