Committee on Information Technology

Total Meetings: 6  
Meeting frequency: As needed  
Average hours of committee work each week: varies

Total Requests for Consultation responses: 4  
Total of reviewed proposals deferred from the previous year: None  
Total proposals deferred to the coming academic year: None

Listing of bylaw changes proposed: None

Listing of committee policies established or revised: None

Issues considered by the committee:
- New Learning Management System (LMS)/Tracking Faculty Time to Learn New System
- BigFix
- UCDNet4
- Email For Life Service Change
- SmartSite Outage

COMMITTEE’S NARRATIVE

The committee met six times during the 2015-2016 academic year. Meetings were scheduled as needed. The Academic Senate Information System (ASIS) was used to notify members and distribute relevant information about the committee’s upcoming meetings.

Below is a brief description of major tasks that the committee addressed during the 2015-2016 academic year.

**New Learning Management System (LMS)/Tracking Faculty Time to Learn New System**

UC Davis IET is working on replacing the current SmartSite with a new LMS system. By Winter Quarter 2017, the majority of the campus will be transitioned to the new learning management system, Canvas. The committee has concerns regarding the faculty time commitment in transitioning to the new system. To capture this information, the committee has developed a survey that can be accessed on the Canvas home page. Faculty will be asked to log the time it takes to transfer their courses to the new system and answer a couple brief questions. This data will allow CIT to understand the time needed for faculty to transition from one LMS to another should such a transition occur in the future.

**BigFix Implementation**

The committee on Information Technology received a consultation request regarding the campus wide implementation of BigFix. BigFix is a system that automatically installs patches provided by vendors. The committee reviewed and discussed the BigFix campus implementation and advised on the policy and procedures for exceptions to installing BigFix. The committee recommended a number of additions and changes, one of which resulted in the policy that “prior to denying any faculty member’s request for a BigFix exception, the Information Security Office will consult with the Academic Senate’s Committee on Information Technology or its designated representative.”

**UCDNet4**

UCDNet4 is the replacement of core components of the University of California at Davis campus data network. The goal is to provide a modern, reliable, secure, and efficient high performance network to support the diverse needs of the campus. IET is currently gathering information and sought input from CIT about the process. CIT has had multiple discussions regarding UCDNet4 and has expressed a few
concerns (such as funding). IET stated that they will be happy to consult with CIT regarding cost and other information.

**Email for Life Service Change**

IET had proposed deactivating faculty and staff email accounts after two years of inactivity, excluding emeriti faculty. CIT supported this proposal given that staff and faculty could re-activate their accounts if desired.

**SmartSite Outage**

In May 2016, the current learning management system SmartSite experienced an extended outage during which students, staff, and faculty did not have access to the system. CIT discussed the causes, effects, and possible solutions with the IET executive team during the last meeting of the Spring Quarter 2016. CIT drafted a letter stating its concerns about the system outage and failure of the disaster recovery plan, and requested that IET provide the disaster recovery plans for faculty-critical systems (such as the LMS) so the Academic Senate could be apprised of them. CIT sent the letter to the Academic Senate Chair, André Knoesen, and the IET executive team.

Respectfully Submitted,

Matt Bishop, Chair  
Giacomo Bonanno, Member  
James Fadel, Member  
Michael Kleeman, Member  
Vladimir Yarov-Yarovoy, Member  
Alex Limon, ASUCD Rep  
Jeremy Lea, Academic Federation Representative
May 31, 2016

André Knoesen, Chair
Academic Senate

Dear André:

The Committee on Information Technology believes it is critical to gather information on the time faculty spend learning to use Canvas, and moving their classes from SmartSite to Canvas. Doing so will enable us to estimate the work load on teaching faculty if, and when, Canvas is replaced with another learning management system. Perhaps more importantly, the data we gather will allow us to calibrate support for the transition as it proceeds, and communicate any issues to the UC Davis Canvas group.

We have discussed this with David Levin, and he has said he will work on developing a method for measuring this effort. However, we are concerned that the method will not be in place before faculty begin to use Canvas this summer or fall.

We therefore propose the following course of action. Provide a link for faculty on Canvas to a database or data collection system where they would enter the following information:

Course name:
Time to learn Canvas:
Time to transfer information or set up course in Canvas:
Time to make adjustments after course is set up:
Scoring:  (1 to 10, with 1 for easy to use to 10 for difficult to use)
Comments:

Also, put the following text on the Canvas page that faculty see when they log in:

“The Academic Senate Committee on Information Technology is trying to determine how much effort is required to transition from SmartSite to Canvas. To help us do this, please keep track of the time you spend learning to use Canvas, the time spent transferring any content from SmartSite to Canvas, and the time needed to make adjustments after the course is set up. Click on the link below to enter that information. Please do not worry about being exact; we’re trying to get a best estimate. We will correlate the results, delete the names, and use this information to determine how best to support the transition of all faculty to Canvas. Thank you.”

and below this text, the link to the data entry system (perhaps https://ucdavis.qualtrics.com if that would be suitable).
Sincerely,

Matt Bishop

Matt Bishop, Chair

C: Giacomo Bonanno
James G. Fadel
Michael J. Kleeman
Jeremy Lea
Vladimir Yarov-Yarovoy
Dear André:

The members of the Committee on Information Technology have reviewed the document “Campuswide Implementation of BigFix” that Mr. Thonen sent to the Academic Senate for consultation. We have 8 suggestions, listed following this letter.

We believe that the composition of the BigFix governance advisory group mentioned in the second bullet of item 5 is critical in determining whether the Academic Senate should support this. In particular, if the Senate has membership and influence on the panel, then the members of the Committee would recommend supporting this after the changes below are made.

1. In line 2 of item 1, “and to and to” to “and to” to eliminate the redundancy.

2. In item 2, lines 4-5, change “Using BigFix more broadly will help UC Davis secure its information assets and comply with laws and regulations pertaining to the protection of personal and health information” to “Using BigFix more broadly will help UC Davis administrators, faculty, researchers, and staff secure their information assets and comply with laws and regulations pertaining to the protection of personal and health information”. This changes the impersonal “UC Davis” to emphasize that security is everyone’s concern.

3. Change the first bullet in item 3 from “BigFix allows the campus to respond quickly in the event of a cyberattack, to identify and protect computers that may be vulnerable, and to repair compromised computers” to “BigFix allows campus security officials to respond quickly in the event of a cyberattack, to identify and protect computers that may be vulnerable, and to repair compromised computers”. Again, it eliminates the impersonal.

4. Change item 5, bullet 1, to the following:

“Will use of the system be mandatory for faculty? BigFix is being adopted as a standard for user system protection at UC Davis, and should be installed on all campus owned and managed desktops and laptops, unless an exception has been approved. Faculty may request an exception by submitting a request to the UC Davis Information Security Office. The reasons include that the faculty member will maintain the computer in compliance with all UC and campus policies and applicable regulations, that the installation of BigFix could compromise the integrity of research, and that BigFix will not run on the endpoint. As an alternative, faculty members may allow the installation of BigFix for reporting purposes only. Additional information about exceptions, including more examples of reasons for those exceptions, can be found in the IT Service Catalog: http://itcatalog.ucdavis.edu/service/bigfix.

André Knoesen, Chair
Academic Senate
Mobile devices, tablets, and servers (e.g. HPC clusters) are not included in the current plans. As noted above, the UCDHS is excluded from the plan.

5. Add the following to the second paragraph of bullet 5 in item 5, “If at all feasible, the owner of the computer will be consulted before software is installed, removed, enabled, or disabled. If not feasible, the owner of the system will be informed of the action and the reason for the action as soon as possible.” This acknowledges the concern of faculty that software incompatible with what is on their system will be installed, while acknowledging that under some circumstances immediate action may be needed to protect the campus and other computers on campus. It also assures faculty that they will be informed whenever a change to software is made on the systems they manage or use.

6. In item 5, bullet 5, paragraph 3, change “can be reported” to “will be reported to the manager of the system on a monthly basis.” This simply assures that the actions taken by BigFix will be reported regularly (as opposed to “can be reported”, which means they may or may not be reported).

7. In item 5, bullet 5, paragraph 5, add “BigFix will not be used to install any software that carries out any of these tasks without the consent of the system manager and without informing the users.” This assures people that monitoring software will not be installed surreptitiously on their systems.

8. To item 5, bullet 6, sub-bullet 1, append “but the implementation of any centralized solution like BigFix makes exercising those rights easier.” This simply acknowledges that centralization (even at the organizational unit level) makes control possible remotely, and hence easier.

We hope this is helpful.

Sincerely,

Matt Bishop, Chair
04/19/2016

André Knoesen, Chair
Academic Senate

Dear André:

The committee on Information Technology believes that deactivating faculty and staff email passwords after two years of inactivity is reasonable, given that staff and faculty can reactivate their account if desired. The exemption for emeriti faculty is appropriate.

Sincerely,

Matt Bishop, Chair
The Committee on Information Technology considers SmartSite’s lack of availability to be a failure of a mission-critical resource of the University.

Many teaching faculty use SmartSite for managing their classes, for example having students submit homework on it, keeping track of grades on it, and returning graded homework on it. In its absence, faculty have had to create workarounds using Sympa, Box, and other tools such as Google web sites.

The Committee has learned that the failure occurred at the vendor’s site, and that the disaster recovery plan assumed that the vendor would provide access to another set of required resources. The University’s disaster recovery plan depended wholly on the vendor. The problem, of course, is if the vendor becomes inaccessible (due to catastrophic network failure, for example) or is unreliable, the University has no disaster recovery plan or capability — and that is exactly what happened with SmartSite.

Exacerbating this concern is the campus’ move to a new Learning Management System, Canvas, during the 2016–2017 academic year. Do this, and other mission critical systems, have disaster recovery plans that depend on external vendors? It is imperative that the University augment any such plans with disaster recovery plans to be used should the vendor be inaccessible or unwilling or unable to recover. Acceptable down time for these mission critical systems must be minimal — in the case of the learning management system, no more than a day.

The Committee believes it is imperative the Academic Senate be apprised of the disaster recovery plans for systems that touch on the faculty’s missions of teaching and research, so that faculty can give input to the suitability of the plans, and know what to expect should a disaster similar to the one involving SmartSite occur. Because faculty members will need time to plan appropriately if an in-house disaster recovery plan for anything other than a fully functional system is not in place, we request a response by August 15, 2016.

We appreciate the difficult situation the failure of the third-party vendor has placed IET in. Our goal is to prepare for another such situation so the impact on teaching will be much less than the current problem, and IET will not be placed in an untenable position again.

Sincerely,

Matt Bishop, Chair
Giacomo Bonanno
James G. Fadel
Michael J. Kleeman
Jeremy Lea
Vladimir Yarov-Yarovoy