Faculty Committee on Educational Technology

Meeting Minutes: October 12, 2011

Officers: Brenton LeMesurier, Chair; Anthony Bishara, Secretary

Call to Order: The meeting was called to order at 9 AM in Robert Scott Small Room 353

Attendance: *Members*: Anthony Bishara, Bob Cape, Deanna Caveny, Morgan Koerner, Monica Lavin, Brenton LeMesurier, Tim Scheett *Guests*: Deborah Johnson, Deborah Mihal, Phil Paradise, Jeff Wragg

Agenda:

1. Approval of minutes from the previous meeting, September 7.
2. Reports:
   a. Report from the committee chair, Brenton LeMesurier.
   b. Report from the CIO, Bob Cape.
   c. Report from the director of TLT, Monica Lavin.
   d. Report from the Provost's delegate, Deanna Caveny.
3. Old Business:
   a. Banner/MyCofC requests and complaints.
   b. Proposal on computer testing center. (Tim Scheett/Deborah Mihal.)
4. New Business:
   a. Resource needs for on-line courses: request from Faculty Speaker Lynn Cherry.
   b. Report from Phil Paradise (Director of Support Services) on IT support.
5. Other business.
6. Schedule next meeting and adjourn.

Discussion of Agenda Items:

2b. IT report – Bob Cape

- CofC continues to experience phishing. IT will have poster campaign to increase awareness.
- IT screens incoming and outgoing mail, and is experimenting with additional screening techniques. There is a trade-off between misses and false positives; screening errors on the side of producing more misses than false positives (to avoid misclassifying valid email as spam).

2c. TLT report - Monica Lavin

- D2L grade integration with banner will hopefully be ready for final grades this semester
- OAKS forums are available for help. TLT is working on a dedicated OAKS blog. TLT has a FAQ for OAKS, and the FAQ address roles among other issues

2d. Provost's office report – Deanna Caveny

- The Provost's office has formed a committee to address online administration of teaching evaluations
- The pilot project for online tenure and promotion packets is proceeding.

3a. Banner/MyCofC requests and complaints.

- The global timeout is to address the issue of students accidentally leaving public computers without logging off. IT is currently investigating whether to allow different timeout periods for different roles (e.g., faculty, staff)

- Network drive back-ups involve 2-building redundancy and once-a-week transfer offsite. College-related work material should be stored on the network drive. Email is not secure.
- Future faculty complaints or concerns should be directed to the helpdesk or Bob Cape.

3b/4a. Proposal on computer testing center (Tim Scheett/Deborah Mihal.)/Resource needs for on-line courses

- If we were to do OAKS testing, CofC's volume needs would be large compared to Trident's. The proposal is shifting toward a more general testing center. The facility could be revenue generating.
- Tim's survey needs to go through the Office for Institutional Effectiveness and Planning.
- A technology needs analysis needs to be done for the space (contact Monica Lavin).
- The testing facility could possibly find a natural home in the new technology building (possibly part of the new master plan).
- Virtual security (e.g., via webcam) is one possible alternative.

4b. Report from Phil Paradise (Director of Support Services) on IT support

- IT support manages helpdesk, student support, telephone services, field support, and special projects.
- Help desk issues are tracked and directed to appropriate offices/individuals. Tracking continues even if the issue leaves the help desk office. Tracking statistics are used to monitor and improve performance.

Decisions Made:

- Minutes approved (for 9/7/11)

Meeting adjourned: 10:00 AM

Next Meeting: November 9, 2011 at 9AM, RSS 353

Approved Minutes Addendum: IT Response to Concerns about Banner and MyCharleston

1. **Time-out on MyCharleston too quick? Allow slower time-out on a trusted/private client, as with WebOutlook?**

   - We are investigating ways to allow longer timeouts per roles (i.e. faculty, employee, student, etc)

2. **Enforced password changing protocol: inconvenient and with some evidence cited that it does not help security. If not eliminated, giving sufficient advanced notice?**

   - Security best practices warrant frequent password changes. With the recent increase in phishing attacks and the number of College of Charleston faculty, staff and students that have responded to the attacks gives even more credence to frequently changing passwords. Many times these hackers sell identity credentials to others and it may be several months before the credentials are used to compromise our systems. Changing passwords frequently helps thwart this. Unfortunately, the time that a password expires is controlled by the application and we cannot modify that. We are investigating publishing in MyCharleston when you first log in, a date and time when your current password will expire. We are also investigating other advanced notification solutions that alert you to upcoming password changes.

3. **Related to the above: Difficult to remember strong password. If we have to change our strong passwords every 90 days we will either make our password into an easily-guessable variation on the last password, or we will write it down everywhere, because otherwise how can we remember it? One remembers one's first password, and maybe one's first fifteen, but it really degrades after that, at least for me.**

    - There are techniques to remembering passwords—think of a phrase, substitute a $ sign for the letter S, instead of an "I" use a 1, etc. When required to change the password, think of a similar phrase or slightly change the original phrase substituting other special characters. More and more of our systems are using the same credentials. It is very dangerous and a risk to the college not requiring frequent password changes. If one would guess your password, one could log into MyCharleston and obtain your bank account number and possibly steal your identity.

4. **Related to the above: enforced Active Directory domain COUGARS password changes do not change passwords for Mac OS X Keychain (or for listserv.cofc.edu, spinner.cofc.edu) potentially requiring a number of additional password updates, or an annoying succession of prompts from KeyChain for Mac OS users. The problem is greatest for faculty who use multiple Mac OS computers in various classrooms, and are thus unlikely to update all the relevant KeyChain passwords immediately after each COUGARS password change.**

    - As stated before, the time that a password expires is controlled by the application and we cannot modify that. We are investigating publishing in MyCharleston when you first log in, a date and time when your current password will expire. You can then be pro-active and change the password ahead of the date and time to prevent embarrassing changing during a classroom presentation. We will make sure information is published on the IT HelpDesk web page regarding changing of keychains for MAC users.

5. **Commas vs semi-colons when emailing a class from MyCharleston**

    - In Banner you have to pick 1 delimiter, either comma or semi colon. Most email clients use commas as email delimiters. Outlook defaults to a semi colon, however allows an option to change to commas. The other email clients to not allow the option to change to semi colon. So the faculty that is using the email distribution lists delivered via SSB need to make a modification to their outlook to allow comma's as separators.

Instructions:
In Outlook 2010, follow the clicks below and “check” the box for ‘Commas can be used…’:
‘File’ tab / ‘Options’ / ‘Mail’ …

Pre-2010 Outlook:
‘Tools’ / ‘Options’ / ‘Email Options’ / ‘Advanced E-Mail Options’
Check ‘Allow comma as address separator check box’

6. **Add a "Major" page to MyCharleston**

   - Web Services is set to create the tab as requested and it will be implemented by Friday Oct 7

7. **Option to display more than 20 students per page in MyCharleston**

   - The SunGard configuration settings allow an institution to specify a global “number of students to display” value, for each of ‘Class List’ and ‘Grading’ pages. Currently, those are both set to ‘20’, as established by the Registrar’s Office. By setting the length to 20 per grading page, instructors are protected from timeouts while grading that might cost them their entered and unsubmitted work. A max of 20 per page means they will have to submit every 20 and can lose no more than 20.
     However, it is a possibility that the number could be set differently for the separate pages (for example, it could be set to 35 for ‘Class List’ and 20 for ‘Grading’).

     Two options that would require local enhancements would be:

     - Allow each faculty member to set their own display number, and save that number for future use
     - Allow each faculty member to adjust the display number, each time they use the page(s)

     Either of these options would mean a time-consuming modification and could result in unintended consequences. This type of change would be more than a minor project and there are currently much higher priority enhancements to make. However, the Registrar’s Office is open to the discussion of maximums with the FETC.

8. **Notification and website download help for replacing software that has security issues, as is allegedly the case with Adobe Reader X, so that reverting to version 9 has been recommended**

   - Information Technology does not manage or coordinate Adobe security updates. Adobe security patches are managed by Adobe and automatically made available to users. Typically when the user opens an Adobe product they are prompted to update. Adobe Reader X is the most recent and secure version. Reverting to previous versions is not recommended. For example, Adobe issued a security alert on February 2011 that stated:

"Critical vulnerabilities have been identified in Adobe Reader X (10.0) for Windows and Macintosh; Adobe Reader 9.4.1 and earlier versions for Windows, Macintosh and UNIX; and Adobe Acrobat X (10.0) and earlier versions for Windows and Macintosh. These vulnerabilities could cause the application to crash and potentially allow an attacker to take control of the affected system. Risk for Adobe Reader X users is significantly lower, as none of these issues bypass Protected Mode mitigations."
https://www.adobe.com/support/security/bulletins/apsb11-03.html

The alert then provided an update that resolves the issue.

9. **When will we move to Windows 7**

   - Currently Windows 7 is deployed at the College of Charleston in very limited numbers and is supported by the Helpdesk on a limited basis. In recent weeks Information Technology has made significant progress in resolving several critical compatibility and support issues with Windows 7. The current deployment plan is to begin installing Windows 7 on all newly purchased computers starting in the spring semester of 2012. Planning for deployment to existing computers is ongoing, but should begin within the first quarter of 2012.

10. **Logging into the IMAP email interface requires password sent in clear text: can an encryption option be added? (An issue in particular for non-Windows (Mac OS and Linux) users?)**

    - Encryption for IMAP is an on-or-off setting. Once it is turned on, every client that uses IMAP must modify their configuration. While this should be possible for the clients we know about, it will cause a support burden.
      We plan to include secure IMAP in the Exchange 2010 rollout, so that we can identify all of the affected users, test representative configurations, document change procedures, and migrate the user base to the new settings

11. **File backups/copying to fs2 from non-Windows computers, where the UNIX-style file permissions used on those computers are sometimes garbled.**

    - This problem might be an issue with that specific PC. We have not heard of this issue from any other Mac users so it might be a good first step to have Helpdesk check that particular computer for issues.

12. **The limitations of the server-based backup options and the recommendation of instead using portable back-up drives create a data security problem (backup drives stored in offices have been stolen.)**

    - IT does not have the personnel or financial resources to conduct backups of each campus PC or laptop. With over 3,500 laptops and PC's and over 430 TB of data to back up, this would be cost prohibitive to have an enterprise backup system to support this large amount of data backups. Users are encouraged to save their work related documents to their shared drive which is backed up by IT. Users should not save work related data to local drives. Mac users can use TimeMachine and Linux users could use a cron job to back up their data automatically but it is **imperative** that they only use it for work-related files and documents and not their system configuration files. Personal photos, personal music, personal videos **should not** be saved to enterprise storage. We have not promoted the general use of external hard drives for work related information as it is not a secure method of backing up data. External drives are permitted only in cases where College related files cannot be saved on network drives.

- Data Center servers are routinely backed up and copies of the backups are maintained in remote locations.

13. Can grading assistants be authorized to post grades in OAKS?

- Students with formal grading assignments are first required to sign a confidentiality agreement and then can be put in the grading role in OAKS. They can then grade assignments (associated with certain tools) that feed into the grade book. Students cannot enter grades directly into the gradebook in OAKS. Our understanding is that they could not be given access to do that without also receiving access to enter new assignments, make adjustments in how grades are calculated, etc. In addition to the grading assistant role, TAs who are formally instructors of record or non-instructors of record (and listed as such on the course in Banner) have full gradebook and grading rights in OAKS and Banner.