City College of San Francisco
Minutes for ITPC Meeting on March 20, 2012

Attendees
Committee Members: Craig Persiko, David Yee, Joe Jah, Anthony Costa, David Hotchkiss, Lidia Jenkins, Peter Goldstein, Ophelia Clark, Shawn Yee
Resources: Carol Reitan, Cynthia Dewar
Guests: James Hall, Tim Ryan,

The meeting was called to order at 1:10 pm.

I. Approval of Minutes
   A. The minutes from 2/21/2012 were approved.
      i. Clarification of the name of ITS was discussed. It was pointed out that the Board of Trustees has the authority to change the name. Dr. Hotchkiss explained that the Chancellor said that the name was going to be changed from ITS to Technology. The change was never made. The Chancellor had confirmed in open meetings that Dr. Hotchkiss’ title would be changed from CITO to CTO.

II. Old Business
   A. Report from Network Security Group (Tim Ryan)
      i. Tim Ryan reported that the ad hoc committee met for Network Security met. Members included Anthony, Joe, and Sam Bowne.
         1. Network Management Procedures were discussed.
         2. Content filtering was discussed. This is a challenging aspect of technology. What becomes apparent is that there are threats to the College systems and there is always a need to be pro-active. We have systems to help with this task. In the past year, year and a half we have blocked blocks of addresses. The committee talked about the impact of releasing these blocked addresses. Specifically, the committee talked about the Millennium system in the library. The network was blocking this system and causing slowdowns impacting the functionality of the library. ITS now block the threats before they get to our firewall. There have been reports of people not being able to access the CMS and there are sites that are not accessible internally. CCSF does not have a way to confirm access from foreign countries. It is possible that there are legitimate users that are attempting to access our site and we do not have control over this type of access. Tim reported that ITS is going to free up the blocking of some of these groups of IP addresses and monitor it. During the period of April ITS will remove some of these IP addresses and monitor it. It is not good practice to lump IP addresses together. All ranges of IPs will be removed. We will monitor and see what needs to be refined. The ISP, Scenic for the State of California, uses 14 days. The other trade-off is staff time. As we become pro-active it becomes almost one person full-time to do this monitoring. Whether there is any
threat or not, it is a manual process and thus time-consuming. We
have all sorts of protection. Scenic doesn’t do any blocking for us.
We do have blocking, our firewall and our anti-virus software.
Committee members asked if there has been any research in
upgrading our systems.
3. We have two firewalls. One of the reasons is that you used to be
able to allow web traffic but now viruses come across the
network disguised. We have a vendor, Dataway, and they will
meet with our security engineer. There are 130 rules with some
complexity. We are scheduling an upgrade to the Checkpoint
firewall. It will require a four hour window when nothing will be
allowed in or out. We are proposing this and will talk about it
further in this meeting. It doesn’t require any hardware. It is a
software update and it will last another year.
   a. The software upgrade was scheduled for Sunday, April 22,
2012 between 8 am and 12 pm. The campus community
will be notified. Tim will put it on the website and send
several emails to the campus community. It was suggested
that there be a splash page with a re-direct to a Google site.
4. We did talk about UDSN and that is an agenda item later.
5. Banner Password. There is no time limit/change cycle for Banner
passwords. ITPC needs to put this into place and talk about the
parameters such as frequency, overall changes, etc. It is good
security practice to put this into a change cycle. Dr. Hotchkiss
pointed out that this is not a one-time action and it does need
policy action. It was suggested that IT make the recommendation
based on workload and security. IT will come up with a
recommendation with parameters with the goal a policy
recommendation forwarded to CAC.

B. Update on Content Filtering Resolution which was discussed last year,
related to recent proposal to block “malicious” IP addresses.
   i. There was a resolution about content filtering that came from the
Academic Senate and CAD. It went to the Board of Trustees to ask for a
policy on content filtering. It went to FIT. Members recalled that the
topic was on the FIT agenda a few times. It was on the most recent FIT
agenda and it was stricken. Dr. Hotchkiss reported that the reason that it
was not voted on by the Board is that content filtering had already been
rededicated. There was no reason to bring it up if it wasn’t an issue. Dr.
Hotchkiss reported that he was sitting with Trustee Rizzo when Rizzo
asked if content filtering. Members indicated that it is important for FIT
to address this policy because it is a policy that preserves academic
freedom and significant changes in content filtering need to be brought
through Shared Governance. Such a policy will help in the future to
address such situations. Even though it is not talked about now, if there
is not a policy then we are back to where we were before. ITPC has the
ability to create such a policy. If there is an action that ITPC agrees on
and it is brought to CAC, it can be put on the agenda for FIT as a discussion item and not necessarily an action item. The committee was directed to the draft of the Network Management Procedures, 3.4. While 3.4 references URL/IP Filtering, there is not a loop back to Shared Governance. For example, that IT makes regular reports to ITPC. It was also suggested that academic freedom and access to information included in 3.4. The content filtering resolution was pulled from the agenda (FIT?) in January. This committee has historically created policy and has the policy gone to the Board? No. So, this particular policy does not necessarily need to go to the Board. A policy has to go to the Board of Trustees if the policy is going to become part of the District Policy Manual.

C. Network Management Procedures draft version 1.2 was discussed with changes made.
   i. Members made comments related to specific sections of the document.
   ii. Dr. Hotchkiss pointed out that the document does not talk about configuration management and documentation. If it is truly a guideline then it should be documented. It could be a separate section under “Configuration Management and Control”.
   iii. It was discussed that some users do disable the anti-virus software because it slows down their computers. Many computers are set to scan on boot up; this can cause delays as the computer is scanned. Maybe the settings could be changed.
   iv. Privately owned computers and network security was discussed related to 2.9. Faculty and staff are forced to bring in their own computers. It was pointed out that ITPC doesn’t know the extent of the network security problem so that it makes it challenging to make decisions on such a polity. Peter agreed that there is an unanswered question at the College. That is not to say that there are not threats in general but if you are part of this College community then there is an expectation that we are given information in order to make decisions. There are 10,000 wall jacks in the district. There are some that are not connected. At Mission Campus, Anthony pointed out that students are directed to use wireless and faculty/staff are directed to use wall jacks. Peter pointed out that there needs to be some expectation and policy. Dr. Hotchkiss raised the question about indemnification and liability. Peter pointed out that the purpose of the document is not to create a legally binding document.
   v. Classroom Access (2.11). It was suggested that it be clarified that access be clarified to faculty and staff. Anthony brought up access in other locations, such as the library. Tim said that it is $100 to pay for the Ethernet jack in the background to connect each jack. IT purchases the connection is bulk. Requests are made based on need. The infrastructure is purchased and turning on the jacks depends on usage in a particular area. Tim pointed out that it is more effective to direct students to use the wireless system.
vi. URL/IP Filtering (3.4). Members suggested that re-affirming academic freedom is included in this section and changes were made to the document.

D. Update on UDSN Report(s) including appendices, which have been reviewed.
   i. The reports are not complete. Peter received them from USDN. He selected an internal panel of six experts adhering to USDNs stipulation. Craig and Tim read the report. It lists incidences in January of malicious activities attempting to access the network. It does not include access to PII. The report came in two deliveries from UDSN. They are not writing any more reports. In terms of the November item, Peter does not have any information. The report was not part of the deliverables in accordance with the UDSN contract. The final report does not cover November and December it focuses on January. Dr. Hotchkiss was asked about the report. So, there was no one that knows about the content of the report. A lot of the documentation was destroyed. The system was unplugged so errors were recorded on the system and the reports were over ridden. Dr. Hotchkiss reported that he gave the Power Point presented at FIT in January is the report by UDSN. The PPT was not a deliverable. Dr. Hotchkiss directed the committee to Scott Dickey. Peter noted that any report presented at a public meeting becomes part of public record. It was on USDNs thumb drive. We are a public institution and we don’t have any proof about this network security instruction. It makes us look bad. Dr. Hotchkiss says that the College lost 3000 pages of evidence by unplugging the servers. DH reported that his technician reported that there was a virus in the lab and it was transmitting data out across the network. It was someone walking into my office and saying, this is what we have. Was there ever a report? It was suggested that the committee is
   ii. Written report related to the closing of the lab and what led up to the closing. Was there any action to preserve some of the logs?
   iii. If the security even happened in November and IDSN advised us to buy the boxes later, after November, I’m trying to get what was turned off. The boxes were not plugged in In November. Howe could something in November be related to some... Evidence from USDN on what the attacks were actually. The Chronicle reported specific details about the attack. Where is that log? If USDN was so thrown together, can we trust UDSN? Otherwise we have a vendor that is saying all these things happened and the vendor still requires payment. It makes us look corrupt, and bad. Something from USDN showing what actually happened. At least, the six people can see the report. Can UDSN really restrict what we do with a deliverable? Peter said that he consulted with Scott, and he has been advised that he cannot make the report public. Dr. Hotchkiss will answer the questions at the next ITPC meeting. It was added that a report be given about the FBI. Peter reported that based on
a conversation with the Chancellor and Dr. Hotchkiss called the FBI. Peter said that he and David called the FBI late in the day.

iv. On January 20\textsuperscript{th} the FBI contacted David.

v. January 23\textsuperscript{th} David called back the FBI.

vi. Dr. Hotchkiss read a statement. When asked for the written statement he said that they were his notes.

vii. Operation Ghost Click.

viii. Frank and Sorenson, and USDN. The FBI indicated that they would talk with other people and that they would be getting more agents assigned. They would be talking to the Attorney General.

E. Update on International Students Lab
   i. JR reported that the lab will be open either tomorrow or Thursday.

F. Report from Email Working Group regarding possible change from GroupWise
   i. Doug Re reported that the group met three times. The goals are to bring costs down and look at a variety of vendors. The group identified 30-35 questions that need to be addressed. It looks like the committee is looking at an early fall recommendation with a spring 2013 implementation. Migration and analogous functions to GroupWise is key to the final decision.

G. Status reports on the Wi-Fi system.
   i. Tim reported that 6452 people have registered for the system. Nearly half the people that have signed up have used it. The highest access is the Rosenberg Library. Access points have been added to the Rosenberg library. The lightest uses are Southwest and Alemany. The Student Union is also in the top five as is the Cafeteria. A student wrote a letter to the editor printed in the Guardsman. And Tim is communicating with that student. The old system does not work and it cannot be turned back on. DH reported that he has a letter that it is in the Chancellor’s office ready to be sent out.

   ii. Dr. Hotchkiss said that we have had four breaches in our network since he has been here. The FBI was first on campus because 13 of our employees information was included on a website. (I didn’t get this part)

III. Reports

   A. ITPC Chair Report – Craig Persiko
      i. No Report.

   B. Chief Information Technology Officer’s Report – David Hotchkiss
      i. Requested that the Acceptable Use Policy be added to the next ITPC meeting.
      ii. The CTO asked if it would be helpful for UDSN to come to the next meeting.

   C. Educational Technology Department Report – Cynthia Dewar
i. Given time constraints, there is no report.

IV. Adjourned at 1:14 pm

Submitted by Cynthia Dewar