CCITP - Meeting Notes
Date: Thursday 4/13/17
Time: 2:00-3:30
Location: TLC 215
Zoom: https://cuboulder.zoom.us/j/198557140

Next meeting is Thursday 5/4

Attendees:
Scott Maize, Sean Pease, Scott Griffith, Gena Welk, John Sibray, Steven Hart, Dan Jones, Joe Workman, Jim Fudge, Chris Bell, Brent Phillips, Jamey Chapin, Grant Matheny, Jeff Taylor, student guest Brooke Langley (IT Student Governance Board), Jamey Chapin, Jacob Tafoya, Aaron Mansfield, Melanie Pappas, Robert Dixon, Debbie Hamrick, Jeff Hoskin

Remote Attendees:
Orrie Gartner, Greg Stauffer, Cindi Lee, David Kohnke, Debra Weiss, Eric Galyon, Jeff Groth, Matt Eberhardt, Ron Richter

Agenda:

	Topic	Time	Speaker(s)
1	Introductions / Agenda Review / Follow-up from last meeting's items	5 min	Chris
2	ITP Profiles	5 min	Jamey Chapin
3	Policy Changes (See attached pdf: AUP Update - DRJ.pdf)	15 min	Dan Jones
4	ICT Procurement Process Improvements	15 min	Chris Bell
5	Discussion of today's topics	30 min	Chris
6	Decision & Action Item Review	2 min	Gena Welk

Agenda 1: Introductions / Agenda Review / Updates on Action Items From the Previous Meeting
(led by Chris)

Item 1: LMS/D2L update
In regards to the LMS (learning management system) evaluation selection process, Jim Fudge reports that 5 vendors responded and it has been narrowed down to 3 finalists:

- Moodlerooms by Blackboard
- Brightspace by Desire2Learn
- Canvas by Instructure

These vendors will be presenting on campus on Friday, April 21:
http://www.colorado.edu/today/2017/04/13/evaluating-our-learning-management-system-campus-visits-and-sandboxes

The LMS will be a phased implementation process to start no sooner than Dec. 2017. It will probably take about 3 semesters to have it fully implemented across campus. (This implementation process includes a migration of existing course content.)

Item 2: Identity management
We will have Kerry Havens, Associate Director for Identity Management, join us next month at the CCITP meeting to walk us through the process of assigning an identikey (in answer to the question - why does it sometimes seem to take so long for my new employee to be issued an identikey?)

Item 3: ITP Portal for ServiceNow
We discussed that perhaps ITP's would like an IT Practitioner Portal for visibility into ServiceNow (the ticketing tracking tool used internally by OIT). Due to a licensing issue this may not be feasible as once was hoped. OIT is still exploring this - Chris Bell will keep us updated as he gets more info.

Item 4: Reminder of format:

- All CCITP participants are welcome to bring up ideas to Chris/Ron/Brent of things they would like to hear more about or have addressed at a meeting.
- Presenters are welcome to bring in information/ideas in draft format - could be useful for ITP's to give feedback to the presenter in this state
- At the end of the meeting, OIT directors (and possibly other speaker visitors) will be asked to leave so we (CCITP participants) can speak candidly about what was discussed.

Item (5): Software Licensing Follow up - Adobe CC and Acrobat Licenses, SQL Server
(Note: Chris accidentally omitted this update at the meeting, but wanted to include it in the minutes for reference).

Updates from Justin Suzuki:

(1) In regards to negotiations for Adobe Creative Cloud and Acrobat licenses, there are no definitive updates yet. However, discussions are happening and they are promising.

(2) "How will SQL Server licenses be purchased and/or offered to campus?"
After further investigation, there is not an easy way to alter SQL purchases to get savings. Therefore, securing SQL server licenses should continue via the usual process.

(3) "Is there a way to streamline Adobe updates for the end user?"
There is an Adobe server application that will do this and it is potentially related to the Adobe Creative Cloud discussions that are happening. No answer yet, but we are hopeful.

Agenda 2: ITP Profiles
(led by Jamey Chapin)

Jamey distributes the "OITWeekly" email each Wednesday (assuming there is content to share that week). This email also includes maintenance items such as upcoming outages.

Question from Jamey, "What do CCITPs want to see in this publication? Perhaps brief profile stories of either CCITPs or OIT ITPs?"

It was generally agreed that readers would like to see ITP profiles in the OITWeekly. In addition to the name, details to include might be: where they work, what software s/he works with, a bio of professional interests and future projects/topics s/he would be interested in working on. It was also suggested that there be info included on their team as a whole and what the department is doing. Question for Jamey: Is it possible to create an accessible archive of these profiles? The ITPs may want to look back at a later date as a resource.

Suggestion for Jamey: The word "maintenance" often shows up in the subject line of OITWeekly. Perhaps it could be changed to reflect more of a unique identifier (such as an included topic from the content of the message).

Agenda 3: Policy Changes
(led by Dan Jones)

Dan reviewed the "Acceptable Use Policy" update (in regards to email).

This question was posed by ERP: Can departments/organizations/units have personnel with different mailhomes: some people using Gmail and others in O365 within the same department? It was noted that it has been hard to collaborate between the different platforms. It was determined this question is for department/org/unit management to decide -- not OIT.

The group agreed with the policy statement.

Question: Can mailhomes be standardized by organization at provisioning? (for example - Can all athletics employees be on one email platform from the date of hire - without athletics IT having to put in a ticket each time to change it from the “OIT standard” to the “athletics IT” standard?) It was noted that the new identity and access management tool will probably be better for this type of thing. Since Kerry will be coming to an upcoming meeting we can ask her this question at that time.

Agenda 4: ICT Procurement Process Improvements

Dan reviewed the ICT Review Procurement Process.
(For reference: http://www.colorado.edu/ictintegrity/
For forms: http://www.colorado.edu/ictintegrity/forms)

- ICT review encompasses both accessibility and security
- “Hardware-only” purchases don’t need review
- Initial review response time is within 2 days
- The whole process should be done 2-8 weeks
- “Resolved” means that ICTReview has “handed it back” to PSC.
- High vs. Low impact depends on the number of people who will be using it, whether it’s assistive technology, or if it is a required element of student participation

Comments by participants:
The review and purchasing process is not transparent to the purchaser. S/he doesn’t have insight into the current stage of the process and has limited methods to determine whether “the ball got dropped,” or other cause which is holding up an approval process.

Purchasers want better communication about the stage of the process at any given time. A ticketing system just for procurement sounds promising. This would offer transparency to the process and documentation.

This review process isn’t ok for many campus departments as it “holds up the whole business process” with critical financial impacts.

ITP’s noted there are too many variables in the ICT Review Procurement Process that need to be synchronized without the appropriate resourcing, causing the frustration for the purchaser. “The core problem here is that this is an unfunded mandate.”

ITP notes that many purchases are automatically flagged that should not be flagged, and many purchases that go through easily should actually require more of a review. For example, those with a Standing Purchase Order (SPO) don’t seem to be flagged for review.

Question for Dan: What are the definitive criteria causing purchases to be flagged for ICT review? Is it a price threshold? A number of users?
If it's price, then theoretically a department could deploy inaccessible freeware to its students...

ITP's would like a clearinghouse (a list of products that have been "cleared" as already being secure and accessible and therefore can be excepted from the ICT Review process) so they can be guided to purchases that will require less effort. Dan says this is one of the longer term goals.

The exceptions process is cumbersome. "The form alone is gigantic." CCITP suggestions for improvement:

- A "save" button on the form so that s/he can return later (without having to re-enter data)
- A branched form methodology - i.e. if the form recognizes that the purchase is low impact, can it "intelligently" navigate only to the needed information?

Some feel that supplemental ICT purchases should not be subject to the same accessibility standards as the primary ICT it exists to assist. (For example, if a supplementary kiosk exists for purchases, then why must it go through ICTReview if the kiosk is a supplement to a human making sales next to the kiosk.) Dan reported that the federal regulations require each ICT be evaluated as a stand-alone item.

ITPs don't feel that administration understands the financial impact to their business or the organization. ITP's would like to know who they can call upon to hear their request for more resources for Dan Jones and his staff.

Questions: When the ICTReview process takes an extended period of time, is there a way to get a solution or a "waiver" for the interim"? If the ICTReview process results in a negative answer, where does the department go for advice on how to act?

Question: Is the contract language that we (OIT) are asking vendors to incorporate in order to comply with security and accessibility standards too extensive? Is this even reasonable?

Action item - Dan Jones says if the ITP's can quantify some of the impacts they are experiencing, he will assist in "getting that in front of leadership."

Question for Dan: Would they (ICT Review board) be willing to implement incremental saves on the exception web form? And also branching on the form?

Action item for Chris: - invite a rep from PSC to attend our meeting

Agenda 4.5: Dan's "public service" announcements

1) The PCI compliance process is happening now. If you haven't been contacted by the security team, please let them know by contacting the IT service desk (help@colorado.edu).
2) Contracts under "Controlled Unclassified Information" - NIST800-171 will have additional security standards to meet.

Agenda 5: Discussion

(No discussion today - out of time)

Agenda 6: Decision & Action Item Review

Question for Kerry: Can mailhomes be standardized by organization at provisioning? (for example - Can all athletics employees be on one email platform from the date of hire - without athletics IT having to put in a ticket each time to change it from the "OIT standard" to the "athletics IT" standard?) It was noted that the new identity and access management tool will probably be better for this type of thing. Since Kerry will be coming to an upcoming meeting we can ask her this question at that time.

Question for Dan: What are the definitive criteria causing purchases to be flagged for ICT review? Is it a price threshold? A number of users?

Action item - Dan Jones says if the ITP's can quantify some of the impacts, he will assist in "getting that in front of leadership."

Question for Dan: Would they be willing to implement incremental saves on the exception web form? And also branching on the form?

Action item for Chris/Brent - invite a rep from PSC to attend our meeting

Questions: When the ICTReview process takes an extended period of time, is there a way to get a solution or a "waiver" for the interim"? If the ICTReview process results in a negative answer, where does the department go for advice on how to act?

Question: Is the contract language that we (OIT) are asking vendors to incorporate in order to comply with security and accessibility standards too extensive? Is this even reasonable?

The following text is the content provided by Dan Jones to which was referred in the meeting: "AUP Update - DRJ.PDF"

B. Privileges and Responsibilities
CU Boulder employees and students are granted access to IT resources and university information based on academic, research, or administrative needs. Access may be suspended or revoked due to violations of policy or abuse of IT resources.

Every employee and student receives an @colorado.edu email account and an IdentiKey, which gives an individual certain access and authorization into electronic resources based on their affiliation (role and status) within the university. Passwords associated with your email account and IdentiKey must be kept secure; and may not be shared with anyone. If you ever suspect that someone knows your password or has accessed your account, change your password immediately then contact the IT Security Office.

Employees are expected to understand their responsibilities also listed in the University of Colorado Providing and Using Information Technology APS [INSERT LINK]. Specifically, the university expects employees and designated university affiliates shall use their official university email account when conducting official university business. Organizational Unit directors and chairs have authority to determine if faculty or staff may have an e-mail redirected to a third party. If technical limitations in an official university email account cause a barrier to an employee performing his or her university duties, the employee shall first consult with the campus IT unit to determine if it is possible to mitigate the limitation. If the OU head determines it is appropriate for the individual to redirect their email to a third party both will acknowledge the employee's responsibilities detailed in APS 6001 section B.1.c.

Employees have the responsibility to protect university information in accordance with requirements and other guidance from the IT Security Office. The employee's responsibility to protect university information also applies to personally-owned computing devices. Private information shall not be stored on personally-owned computing devices unless specifically justified for business purposes and adequately secured (as per guidance from the IT Security Office). IT service providers and other employees with privileged accounts will have additional responsibilities and should consult with the IT Security Office.

Technology that enables collaboration (such as calendaring, messaging, document sharing) may require standardization witching an Organizational Unit (typically a department with an independent budget represented in the Finance System). Directors and chairs have the authority to determine the extent of standardization of collaborative technology is required within their unit. For example, if collaborative calendaring is deemed a requirement for a unit, the University expects faculty and staff of the unit will use their collaborative calendaring to maintain their free/busy availability times, respond to scheduling requests in a timely fashion, and coordinate meeting times with others.

The University may access and disclose employee or student individual content when the University deems a legitimate and appropriate business need. Access and disclosure of content can occur without the consent of the user as long as the protocol outlined in Section D of this policy is followed. Privacy and/or confidentiality should never be assumed in electronic communications.