CCITP - Meeting Notes

Date: Thursday 11/16/2017
Time: 2:00-3:30
Location: ARCE 646
Zoom: https://cuboulder.zoom.us/j/593220113

Next meeting is Thursday, February 1, 2018
--HOLIDAY LUNCH-- on Dec 7 11:30am-1:00pm

Attendees: Melanie Pappas, Gena Welk, Jerry Spivey, Dan Herrick, Chris Bell, Erin Frazier, Dan Jones, Mike Burr, Grant Matheny, Joe LaConte, Brian Radke, Patrice Thoreson
Remote Attendees: Chuck Fischer, Brent Atchley, Todd Schaefer, Greg Hoppes, hoskin, Josiah Workman, Jeff Taylor,, Julian Andrews, LeCarla, Scott, Scott M, Sean Pease, Steve Hart

Agenda:

	Topic	Time	Speaker(s)
1	Introductions / Agenda Review / Announcements	10 min	Chris Bell
2	Acceptable Use Policy / Electronic Communications Policy	25 min	Dan Jones and Erin Frazier
3	Recommended and Supported Hardware and Software	25 min	Dan Herrick and David Cavalieri
4	Discussion of today's topics / Plan CCITP Holiday Party	20 min	Chris Bell
5	Decision & Action Item Review	5 min	Gena Welk

Agenda 1: Introductions and Announcements

(led by Chris)

Previous action items:

Follow up on question: Can the Cisco URL filtering link decrease in size?
Answer: Dan says they are still working with Cisco on how to make the URL shorter. This will improve over time as it is a machine learning process (incorporating “approved” URL’s to a known list).

Action: Dan will supply to CCITP a document his team wrote for BFA to describe WHEN emails get filtered.

Question: Melanie - can we extend the OIT Weekly readership to other key stakeholders? I.e. others in her department to whom it might be relevant.

Action item: Agenda item for discussion at future meeting: How can our (OIT) communications be improved to CCITPs - what kinds of things do CCITPs want to know and how often? How can our Comm staff ensure the right people are getting the communications?

Reminder: Here is how OIT Communicates with IT Practitioners:

OIT Weekly email
To get on the list, click “Submit your Information” on this page:
https://oit.colorado.edu/about-oit/oit-campus-outreach

OIT News
To see the main headlines go to the OIT news page:
https://oit.colorado.edu/news

OIT Service Alerts
https://oit.colorado.edu/service-alerts

To subscribe to OIT Service Alerts and News, go to
https://oit.colorado.edu/subscriptions

OIT Home
https://oit.colorado.edu/

Agenda 2: Acceptable Use Policy / Electronic Communications Policy

(led by Dan Jones and Erin Frazier)
(AUP is attached at the conclusion of the minutes. E-Comm Policy not included.)

Erin is program manager for e-communications tools.

Erin and Dan reviewed:

1. the Acceptable Use Policy Update (9/27/2017)

2. E-Communications Policy and Procedure (Nov Draft)

Changes include:

- “Common set of directory information” - removal of student physical addresses in public directory information
- Supervisors now have the choice to determine mailhomes for their unit (Gmail or O365).
- Upon an employee’s departure or medical leave, supervisors may have “delegated access” to communication accounts.
    - LeCarla asks: will this have to be in writing?
    - Answer: Dan says existing process is that it is required in writing.
        - LC: Will it publicly be clarified that it must be in writing? Dan says yes.

CCITP question: What is first party and third party in terms of email account?
Dan says third party is “not owned or controlled by the university” and he will clarify this in the document and policy.

CCITP question: In terms of “mass” and “bulk” communication, consolidation of these definitions would be useful. What is the threshold? 200? 1000? Is it determined by technical limitation or by impact? Answer: Erin says more work to be done in this area.

Question for follow-up: What timelines may be expected for MOUs and exception requests submitted from ITPs to Erin/Dan? What information should the exception request contain?
Erin will work on what an “exception” request would contain.

Comments and questions? Please contact:
Erin.Frazier@colorado.edu
Dan.Jones@colorado.edu

Agenda 3: Recommended and Supported Hardware and Software
(led by Dan Herrick and David Cavalieri)

Acrobat 11 is EOL as of Oct. 10. (1500-2000 licenses)

$80/person to replace the software (for a 5-yr lifecycle - includes updates)

CCITP suggests Phantom PDF from Foxit software ($9/yr/user for faculty and staff for a subscription model)

CCITP question from remote attendee: “Why not expand the freeware alternatives listed on the OIT software site instead of dealing with Adobe?”

David answers: Because of compatibility and supportability.

More formal and thorough evaluation is needed before campus advertises use of freeware along with campus endorsement. OIT tries to only support products they have the backing of. (So they can contact vendor when problems arise.)

Action item: DC to look into Foxit solution

Office 2011 for Mac went EOL in October.
OIT websites now reflect that this is no longer a recommended or supported solution.

Yosemite Mac OS 10.10 is EOL with introduction of High Sierra. No longer supported by OIT.

10.12 High Sierra - 2 issues:

1) Endpoint protections suite for Microsoft (antivirus for mac) needs to be reinstalled (see the OIT website)
2) Cisco VPN might break during High Sierra upgrade

Action LeCarla - users need to uncheck certain options during High Sierra upgrade due to error messages with VPN. See notes at the end of this document

Windows 10 build 1511 went EOL in Oct. No longer supported by MS. 1511 is extended through March of next year (for enterprise version only). 1607 also ends at this time. Update your fleets by the end of March 2018!

Dan Herrick speaks and presents 2 tablet options by Dell that OIT will be supporting.

OIT recommends Dell tablets instead of SurfacePro, due to

- purchasing strategy campus-wide
- ease of support through Dell

You can still purchase the SurfacePro, but these two Dell models are recommended.

- Performance is equivalent.
- Durability - don't know yet. SurfacePro equivalent is confirmed just as durable.

Dan Herrick would like for you (CCITP's) to let him know when you are having trouble with Dell support. You can leverage the university purchasing strategy with Dell and Dan can help advocate for/with you.

FYI: Dell docking stations have a global shortage. Delays from 1-2 weeks for thunderbolt dock, and up to 30 days for other docks. There are alternatives (third party) docking stations but Dell is preferred.

MS EES agreement. We are in final stages of renewal process. If you use Windows server or SQL you may be able to improve pricing by 4-5%. Email to inquire: Sitelic@colorado.edu

Mdop suite (mgmt tools for windows) is now included in the new EES agreement.

Note from Dan:

> *Confirmed: We don't need to pay for MDOP.*
>
> *MDOP is included with any Windows bundle purchase that includes Software Assurance, and we are purchasing the Desktop bundle. So, MDOP is included. This is from our (Insight) vendor and from the MS Licensing website.*

You should look at (on the OIT website) Recommended hardware:

https://oit.colorado.edu/software-hardware/recommended-software-and-hardware-list/computer-recommendation
This is updated quarterly.
Please go through this and let Dan Herrick (Dan.Herrick@colorado.edu) know what you think.

Action item for CCITP's: This [list at the above link] is intended to be comprehensive of the campus community so they do want to hear your opinions (in representation of CCITP's)

Agenda 4: Discussion of today's topics / Plan CCITP Holiday Party

Holiday party on Dec. 7th?
Yes (according to folks in the room)
Please submit RSVP's to Chris (cbell@colorado.edu) or Gena (Gena.Welk@colorado.edu)

Give feedback to Erin and Dan regarding E-comm policy and AUP. Either through Gena and Chris or directly to them.

Action item: Grant would like to see the policy again after CCITP feedback has been incorporated. (it can be an email - does not need to be an official CCITP meeting item)

Melanie says their (DC and DH) work is greatly appreciated.

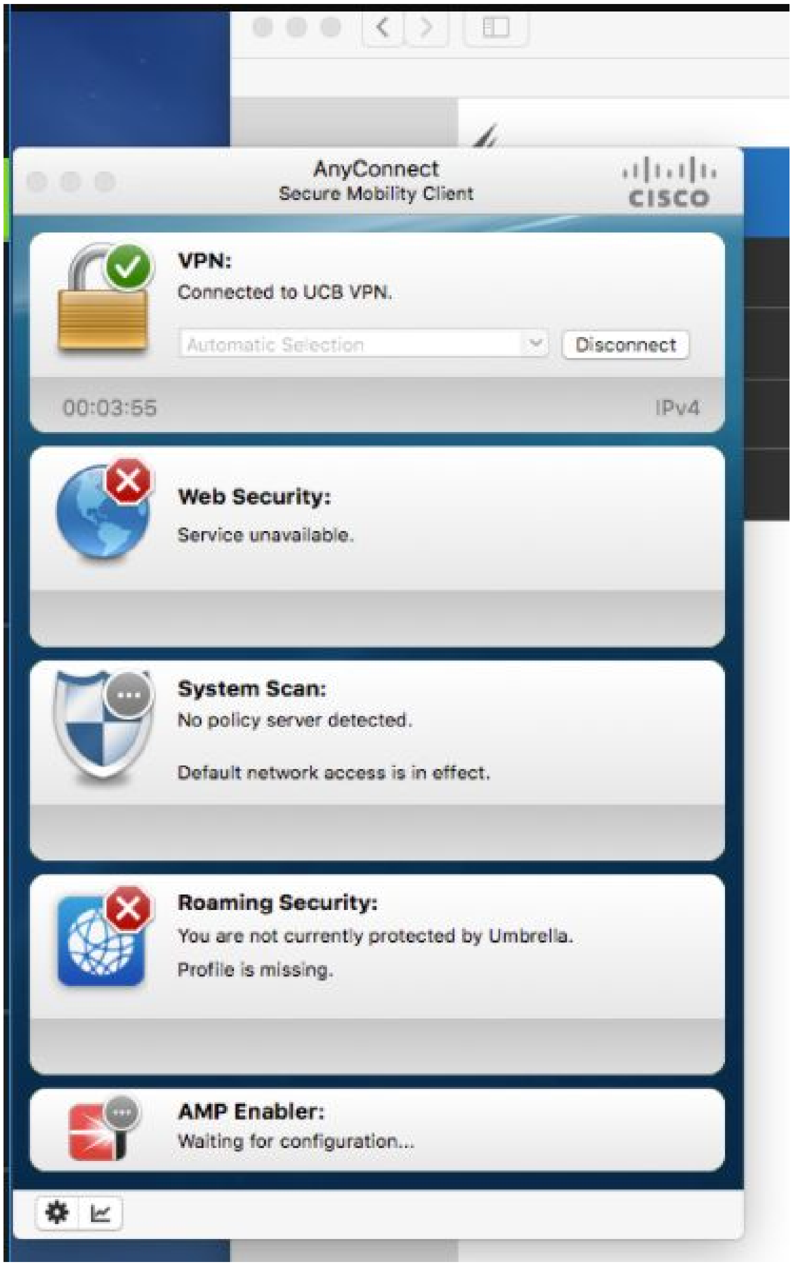
Agenda 5: Decision & Action Item Review
Note from LeCarla at ITSC:

The following options (see image) need to be unchecked when setting up the VPN, which are checked by default in High Sierra:

- Web Security
- Roaming Security

- AMP Enabler

Let me know if you have any questions – Cheers, LC



VPN:
Connected to UCB VPN.

00:03:55 IPv4

Web Security:
Service unavailable.

System Scan:
No policy server detected.

Default network access is in effect.

Roaming Security:
You are not currently protected by Umbrella.
Profile is missing.

AMP Enabler:
Waiting for configuration...

-----------------Minutes are concluded--

-----------------Attachments to Follow: AUP Update 9/27/2017 ------------------------------

Changes to Acceptable Use Policy

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 also expected to understand their responsibilities listed in the University of Colorado Providing and Using Information Technology policy. In particular, the university expects employees and designated university affiliates to use their official university email account when conducting official university business. Organizational Unit (OU) directors and chairs have authority to determine if faculty or staff may have their e-mail address redirected to a third party. If technical limitations in the university provided email account cause a barrier to an employee performing his or her university duties, the employee will first consult with the Office of Information Technology (by contacting the IT Service Center at help@colorado.edu or 303.735.HELP) 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 the employee and OU head will acknowledge the employee's responsibilities following the Office 365 exception process.

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 within 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 required within their unit.

Employees sending *official mass electronic communications* are expected to understand their responsibilities listed in the University of Colorado Electronic Communications policy. To ensure that employees meet their responsibilities the campus provides the eCommunications Central platform. eComm is the preferred university system for mass electronic communication and provides communication tools that meet both business needs and our obligations related to imperatives in compliance, user preferences and data currency/accuracy. Organizational units not using eComm for bulk email or mass audience send will conform to the University of Colorado Boulder eCommunications Procedures and Guidelines.

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.

D. User Expectations

As stated in Section B, the University may access and disclose employee or student individual content when the University deems a legitimate and appropriate business need and those instances are documented and approved by the appropriate authorities. In those instances, if it is necessary to access individual content on IT resources without the consent of an individual currently affiliated with the University, approval must be obtained from the appropriate authority or his or her designee. In the case of faculty and staff working in a school or college, this is the Dean; for all other staff, the Divisional Vice Chancellor; for undergraduate student users, the Dean of Students; and for graduate students, the Dean of the Graduate School. Individual content may be accessed without the consent of the user to comply with legal requirements (including, but not limited to, subpoena, court order, e-discovery request, and/or open records request) as determined by University Counsel. Departmental supervisors may request access to individual content when an employee retires, is terminated, unexpectedly passes away, or otherwise leaves the employment of the University. In the event of a medical, family leave or employee separation, supervisors may request delegated access to employee calendars and request out-of-office messages.

If emergency access to individual content without the consent of the users is required to preserve public health and safety, or preserve the integrity of IT resources and campus facilities, notice shall be provided to the campus IT security principal, notifying them of the need to access files. The campus IT security principal can also assist in obtaining files. All instances of access will be logged by the IT security principal.

Individual content may be accessed through automated information security systems (such as antivirus software, intrusion detection systems, and/or data loss prevention systems) for the purposes of detecting and responding to threats to campus information resources. Excluding client antivirus or antimalware software, the campus IT security principal must authorize all automated information security systems that systematically access individual content. Automated information security systems will log only individual content needed to respond to and identify incidents.

Other than backups for disaster recovery purposes CU Boulder does not systematically archive contents of email communications. CU Boulder, at the direction of University Counsel, arranges ongoing archival of email accounts as required to meet legal requirements.

Add to definitions:

Bulk email: *electronic communications to an audience larger than 200 recipients*

Mass audience send: *any email or other electronic communication sent to 1,000 or more recipients pertaining to university business.*

Official Mass Electronic Communications*: any email or other electronic communication sent to 1,000 or more recipients pertaining to university business.*