In attendance

- Ian Walls
- MJ Canavan
- Ernie May
- Steven Brewer
- Julie Buehler
- Dave Hart
- Charles Mutigwe
- Janine Solberg
- Jon Olsen
- Bret Holloway
- Claudia Donald
- Joanne Gray
- Alyson Gill
- Nikki Stoia
- Jake Cunningham

Announcements

Strategic Planning

Strategic plan still moving forward, with the committee working on stitching together subcommittee documents over summer, possibly with grad student assistance. The CIO requests names of any interested graduate students.

Document identifies current state, future state, action plan as major areas. Styles of subsections vary by group. Working to identify metrics and obstacles.

Video streaming

Video streaming in the future; currently doing testing. There is no offering this year.

Info security

On March 7, there was a major security breach. We hired an external company to investigate, and their investigation so far indicates the problem was phishing. This necessitates more education, as phishing is a much more complex issue than some other security threats. Some of our peers are trying false phishing attacks (with warning) that point to education materials. An interesting idea, but not one we’re planning on at this time.
These security breaches are incredibly expensive.

Information security policy forthcoming. Will call for embedding ‘info security liaisons’ throughout the institution, sometimes paid, officially acknowledged by title. Responsibilities include training and being on-call on off-hours. We first need to build a training program and secure a funding source before we can move forward. For info security liaisons, administrative assistants are often good choice.

Educause has excellent library of security training materials. IT can facilitate usage of these materials within units. Please send any training opportunities within units that are open to wider audiences to the Tech Talks calendar.

Pleasant IT surprise
Vendor who taught online classes had 12,000 Bose headsets to donate (valued at $35 each), UMass just had to receive and process them quickly. Being distributed to many different areas.

Whitmore battery
On April 14th, the campus experienced a massive network outage (¼ campus). An IT team member was injured in the process, but is thankfully doing well.

Eight major network sites around campus are being replaced. The malfunction was in Whitmore, which was already scheduled to be replaced within the year. Debriefings to follow this week.

IT Controls
System controls are being developed following data classifications. IT is working on a baseline set controls for computer systems. The following core critical controls have been identified:

- anti virus
- critical patching
- systems inventory
- encryption
- firewalling

It will be looking more at ‘ghosting’ as a technique for implementing these controls. Apple has traditionally fought against ghosting, as they want users to have the out-of-box experience. This has improved slightly over time.
Staff and student computers also need to fall under IT controls.

**Question:** Is there a universal administrator account for university computers? How do you get into a device if the owner dies?

**Answer:** Some vendors have master passwords to some devices. Departments sometimes set up admin accounts, but there is not a campus-wide solution at this time.

To ensure regular device upgrades, IT is working to identify 2 annual buying times, consolidate purchases to those times, and get to replacements on a 4 year cycle. The aim is for 90% coverage with 7 selected devices (4 PC, 3 Mac). An exception process must be in place for researchers and other who have special needs.

Some researchers have critical research devices running on out-of-date systems, but won’t put security practices on them. One innovative solution that works: if you follow security practices, the Provost will pay for investigations of security breaches, otherwise they come out of the school’s budget.

**IT Security Policy**

There are 2 IT policies under the Confidentiality Policy: acceptable use and information security. Since 90% of questions relate to acceptable policy, that policy was developed first. For information security, start by identifying different levels of information, then how to deal with them appropriately.

**Track changes in policy documents (or diffs)**

There is already an interface to show who made which changes, but its not always the cleanest view. Policy document iterations could be links to Google Docs w/comments, along with a date/timestamp for the version.

**Questions**

**Q:** Where should we look for policy documents around web tracking for marketing purposes?

**A:** Still new, but some analog regulations exist and can be translated from acceptable use policy.

Concerns expressed about relationships with vendors and how they handle our data. Increasing flexibility
is added to our new contracts to allow for changes and shifts in technology during contract term.