Group: Information Technology Council
Subject: ITC Report for 2019-2020
From: Andrew H. Fagg (fagg@ou.edu)

Incoming chair: will be decided at our August 17th meeting

Key issues that the ITC worked on during the 2019-2020 AY:

- **Legacy OU System Accounts (including email)**
  - OU domain email (ou.edu) are subject to per-seat costs (due to migration several years ago to Microsoft) and to the added costs for freedom-of-information act requests.
    - IT is also concerned about compromised accounts.
  - OU employees will be migrated off of the OU email system after they leave OU. For staff, there is a short grace period; faculty have 1 year. After migration, there is no forwarding from the old email address
  - Emeritus faculty will keep their OU accounts
  - Former employees who continue to perform service to OU may keep their email account. This account must be sponsored by a unit and is reviewed annually
  - Retirees will maintain their guaranteed benefits (other than the promised email account). Specifically, an OU system account is no longer required to access these benefits
- **Standardized Computing Requirements**.
  - IT requires us to purchase computing systems (laptops and desktops) from a small, standard menu. This makes system maintenance easier and puts OU in a better position to negotiate better pricing
  - The menu is revisited annually
  - Exceptions are possible, but must be justified
    - "Standard" exceptions: small changes to already available systems
    - Other exceptions: must show that the standard systems do not satisfy the research/teaching needs
  - Having more than one computing device requires an exception
  - Continuing concern: there seem to be some cases where exceptions requests are being denied somewhere between the faculty member requesting the exception and the IT personnel who are evaluating the exceptions (perhaps unit IT personnel or IT personnel that are assigned to units)
  - Continuing concern: the exception process is additional work and adds delays
- **Multi-Factor Authentication.**
  - IT rolled out MFA for access to some systems on campus. When logging into these systems, the identity of the user is confirmed via independent means. There are several options, which seem to cover all use cases
  - In general, the roll-out has been smooth. IT seems to have dealt well with individuals who experienced difficulties
  - The number of systems requiring MFA has been increasing over time

- **Single-Sign-On and Passwords**.
    - IT has been centralizing the system authentication process using SSO. This simplifies user access and can improve system security
    - IT currently requires that the SSO passwords be changed annually Communication and implementation of this requirement seems to have gone smoothly. IT recently proposed reducing the period between password changes. They received very strong negative feedback and an array of published papers on this topic. They seem to have backed off from this plan (we will follow up)
- **Policy, Standards & Procedures Proposal Program**. IT now publishes proposals for policies, standards and procedures at a central location, making them available for review by the OU community, including the ITC
    - Site: https://share.ou.edu/sites/OUITSystemSecurity/_layouts/15/start.aspx#/SitePages/OU%20IT%20System%20Security%20Policy%2C%20Standard%20and%20Procedure%20Request%20For%20Comments.aspx
    - Concern: proposals can be published during the summer
    - Concern: documents are written by and for lawyers
    - Concern: it is not always clear who the responsible actors are when a new policy/standard/procedure is put into place
    - We need accessible mechanisms for disseminating new policies, including clear statements as to who the responsible actors are and what they must do
- **Software for Educational Support**
    - Licenses for software that we rely on have been cancelled without discussion or warning. Examples: Respondus and Gradescope
    - IT and the Provost's office should be involving the ITC (and others) in these conversations. They seem to have acknowledged this
- **Classroom Technology Upgrades**
    - IT has a continuing process of upgrading classrooms with modern projectors and computer interfaces
    - They try to adhere to a standard configuration (though this standard evolves in time). Currently, Apple TVs are not part of this standard, though some rooms have them
    - The current thinking is that we have plenty of active classrooms
- **Health Savings Accounts**
    - Our new HSA provider forced some employees to use their SS# as their account name. This is problematic from the perspective of security of information
    - Employees can ask for a change by calling HSA bank
    - HR is moving to eliminate this option for new accounts
- **Email Filtering**
    - IT has a range of filters on incoming email. Messages that do not pass the filters are thrown away

    - Concern: legitimate communication can be filtered. For example, students who email code when asking for help from faculty or TAs. In other words, entire classes of communication are eliminated & require us to use more cumbersome modes of communication
- **Online Teaching Support**
    - IT upgraded the connection to the Internet, including improving the VPN bandwidth. These held up well during late Spring
    - Zoom largely held up in the Spring. Additional security requirements were put in place during the latter part of the semester
    - While some faculty experimented with doing exams using Respondus, this was not a uniformly good solution (in particular, not all students had the required hardware or bandwidth)
    - Zoom recording: automatic captioning support on mymedia.ou.edu
    - Some students disengaged from classes after Spring break. IT was able to identify these individuals & student services was to follow up with them

Open issues that we are working on for the 2020-2021 AY:

- **Cybersecurity and End User Device Security Proposals**
    - Requires review of non-standard devices being placed on the network. It is unknown what restrictions will be put in place
    - All purchased systems and services require a security review. We have concerns about the expertise and the available personnel to conduct these reviews
    - University-owned devices must be managed by IT. While this might be feasible for standard systems, we have concerns about requiring custom research- or teaching-oriented systems. Some require very specific system configuration (and changing these configurations could make the system non-functional); others don't have typical OSes that can be managed. We are concerned about IT not having the personnel or expertise to do this on a large scale. We are also concerned about the impacts on system performance and on the security of protected data
    - University-owned devices must be kept up to date with respect to current software (especially when security is a concern). Custom systems often have a large number of dependencies. Arbitrarily upgrading a system without understanding these dependencies can make it dysfunctional
    - University-owned devices must have "End-Point Protection Software". This is not feasible on all systems. And, what this entails is not defined
    - University-owned devices must use SSO-based authentication. Many of our systems are not always on the Internet (let alone, the OU network). Examples include: laptops, field-deployed systems, and systems that must be accessed by non-OU personnel (e.g., research collaborators)
- **Sharing of Data with Other Institutions**. We need secure ways of sharing data with our research collaborators, including HIPAA protected data. OU doesn't have these

latter capabilities in-house, and so far is resistant to signing-up for 3rd party services that provide these protections (I have recently secured access to Databrary, but this is an exception, not a generally available solution)

- **Research Computing Requirements**. IT has yet to publish a set of requirements for research computing purchases.
    - Concern: IT is intervening in the purchase process and overriding the decisions that are made by the unit IT experts. This is happening even in cases where an existing computing system is being augmented, for example, with additional storage space
    - Concern: IT requires review of research computing purchases. This adds delay to the process (we have seen delays of many months)
    - Concern: IT has started requiring that new research computing systems be installed in their data center in 4 Partner's Place. This is happening, even when there is space in existing unit machine rooms. Unit IT admins no longer have direct access to their computing systems (except under escort). Data packets moving between the Weather Center and 4PP are routed through Tulsa, which impacts large file transfers.
- **Online Teaching**.
    - Feedback from students for after the Spring semester transition: because every faculty member made different choices for presentation of information and for handling assignments, it was very hard for the students to finish out the semester. This is a continuing concern as many classes will be on-line and all may move on-line for Fall
    - Concern: we do not have a clear path for conducting on-line exams
- **Research Computing Support.**
    - IT is working to bring OU-Norman and OU-HSC efforts together for research computing, storage and backups
    - IT is working toward having firewalled areas for the supercomputer and associated storage for HIPAA and other sensitive data
- **Cloud Computing Services**.
    - OU purchasing has started rejecting purchases of cloud computing services (Amazon Web Services and Google Cloud). These are legitimate research and teaching tools
    - IT is working toward having an agreement with AWS