Information Technology Council Report

AY 2021-2022
Andrew H. Fagg
Chair, ITC
School of Computer Science

Email

- Three years ago: staff and faculty who leave the university will have their email addresses disabled
    - Faculty have a one year grace period; it is much shorter for staff.
    - Emeritus faculty will continue to maintain their email address.
    - For those who are continuing to perform services for the university, they are able to maintain their email address if a sponsoring unit requests it. This extension is reviewed annually.
- New email policy is currently being discussed:
    - All university business over email must be conducted through the OU email system.
        - University business seems to be defined as anything that touches OU in some way. This seems to include conversations with granting agencies, with journals (submissions and reviews), with professional societies and with community service organizations.
        - Communication with and by students is apparently covered, as well.
    - Concerns
        - Poor performance of the OU servers.
        - Delayed support for non-Windows-based clients. These delays can be on the order of years.
        - Email filtering rules drop critical messages from students without warning or error messages.
            - In CS, it is common for us to exchange code by email (this is *much* more convenient than other forms of code exchange when helping students with quick coding questions). However, many of these messages are dropped without error by the OU servers.
        - Faculty professional lives are bigger than our service to OU. Our network-based identities need to be persistent across all of these activities and across time (including beyond our formal association with OU). Hence, faculty are encouraged to establish non-OU email identities. But, this is in conflict with the coming requirements that all OU-related traffic be through the OU email servers.
        - Faculty/staff should not be responsible for enforcing the rules about OU email. For example, what happens when students send email from non-OU addresses?
- Phishing testing
    - OUIT catches ~90% of phishing attempts before they reach our mail boxes

    - Individuals need to be wary of the content of email, including opening of pdf files and the web links that are included in email and contained documents
    - Outlook has a ‘report phishing’ button that can be used if someone suspects that an email is a phishing attemp
    - In testing, OU Norman was at ~7% ‘gocha’ rate. Industry standard is 4%.
    - Individuals who open offending pdfs or web links are required to participate in additional training and are subject to an even greater number of ‘gotcha’ probes.
    - Concerns
        - Tools for detecting/reporting offending pdf are not available for all email clients.

Security Policies

- OUIT has been proposing a range of security policies that can affect research that is done by many groups on campus. Includes:
    - How we access our computers from off campus.
    - How we secure our data.
    - How we share data and computing with collaborators on and off campus.
- New end-point device policy (desktops, laptops, etc.)
    - IT expects to have admin access to all machines.
    - IT will be installing software updates and executing scanning tools.
    - Personally owned machines are expected to satisfy all security requirements. No policing by OUIT is planned for these machines. But, OUIT has been explicit about individuals assuming the risk for lost data.
- Encryption
    - All portable storage devices must be encrypted. OUIT has a central key escrowing system for this.
    - We have had one incident already where many individuals were locked out of their encrypted files for multiple days.
- Multi-factor authentication
    - Generally, seems to be working well.
    - Expect continued expansion of its use.
    - Moving from Duo to Ping
- OUIT will be hiring more staff to address security.
- Passwords
    - Small change to password requirements.
    - Passwords must be changed at least once per 365 days.

Student Issues

- Computers not subject to security requirements.
- OU has transitioned over to using electronic ID cards (called “Mobile ID”). Some faculty do not accept these as valid IDs for entry into exams.
    - Virtual card readers are available through the Sooner Card office for this authentication.

- MyMedia videos that are recordings of a class cannot be used outside of that class. This is being done to protect the privacy of student participants at the cost of being able to use videos in other contexts.

General Issues

- Preferred names: everyone has the ability to specify a preferred name in accounts.ou.edu. IT is working to have various OU systems referred to this preferred name rather than one's given name. If a user finds a system that uses their given name, they should contact OUIT.

Communication

- Trying to figure out how best to communicate to all faculty about critical issues. Seem to be settling on a quarterly email message.
- Also willing to visit individual units to discuss OUIT policies and challenges.

IT Governance

- New committees are being set up for IT governance. Seem to be about making policy decisions. ITC only plays an advisory role, so we are not part of this process.
- Faculty senate has already appointed a member to the Teaching & Learning committee.
- Expecting a Research committee to start soon.
- External review panel for research computing has been convened; will visit in July.

Computer Purchases

- Restrictions on purchases have been relaxed, specifically for externally provided funds and some internal funds (e.g., start-up packages)
- Some restrictions for what hardware can be purchased. These stem from federal requirements.
- Supply chain problems still delaying purchases & will continue to do so for a while.
- Purchases of Apple computers are no longer being held up (there was a prior concern about a security bug in the M1 processor).
- Approval process for non-standard computing purchases is opaque. There seems to be a long chain of individuals that must approve purchases, but faculty have no way of tracking/facilitating progress through this chain.

Supercomputer and Associated Services

- OURdisk: central harddisk system that is maintained by OUIT. Cost to start is just the purchase of the disks; OUIT handles installation and covers cost of power/cooling/maintenance.
    - Can be mounted on supercomputer or computers external to OUIT, but unclear that both are possible simultaneously.
    - $860 / share (10 TB)
- OURstore: central tape backup system. Cost to start is just the purchase of the tapes. $50 / share (7.65 TB)

- OURcloud: cloud computing nodes. Just have to buy a share of a computer. $347 / share
- New supercomputer is coming online now; ready for general use in the Fall. Includes many new GPUs.
    - Flash disk cache
    - Groups can purchase computing that is part of the supercomputer, but is reserved only for their use
- Globus: new service for exchanging large data sets with those from outside OU.
- Support for HIPAA and other sensitive information coming in 2023 (both storage and computation).

ITC Membership

- One current ITC faculty member left the university in December 2021 and needs to be replaced: Sam Workman (term: 2021-2024)

Next/Continuing Big Tasks

- Getting Research and Teaching use cases in front of the key IT decision makers.
    - Need to be clear about what our requirements are.
- Develop a vision for Research Data. What should OU be doing with respect to managing, securing, backing up, sharing research data? Are we satisfying obligations to funding agencies for making code and data available?
- IT Policies and Standards are written with very legalistic language. To those outside of IT, it is often unclear who the actors are and what they are required to do. We need to bridge this gap if these are going to have any meaning.