Group: Information Technology Council 2020-2021
Subject: Minutes for the ITC Monthly Meeting
Date: Monday, August 23rd, 2021, 8:30-9:30am
Location: Zoom

Recorder: Aaron Biggs
Attendees: Andy Fagg (Computer Science), David Horton (OU IT), Aaron Biggs (Provost Office), Nick Key (OU IT), Aaron Baillio (IT), Edward Reali (SGA), Konstantinos Karathanasis (Music), Daniel Deering (VPR), Eric Boyd (EM)

Review of April Minutes - Andy Fagg

Computer Purchasing - Nick Key

- Status of supply chain
  - This is just reminder of the issues OU is having with procuring technology
  - Global delays related to chip shortages and other supply chain issues. Affects anything with a chip including monitors, cables, etc...
  - If you need equipment, talk to IT as soon as possible to work on an ordering strategy
  - IT does have some limit stock
- Apple M1 processor and Big Sur
  - Big Sur is the security software
  - Ordering M1 processors is still “on hold”
  - Can’t install enterprise AV yet due to incompatibility
  - In the Spring, the decision was made by IT security governance review board to place these orders on hold
  - If you have a specific need, especially if no protected data will be accessed or stored, reach out and let IT know. They have some options, but have to look at the specific use case so they can put in the proper controls.
  - IT is planning to send out back-to-school email about computer standardization.
  - Andy Fagg - I was able to buy multiple machines with external grant funding. Process is working well.

Authentication and Password Policy Implementation - Aaron Baillio

- Password Policy
  - New password requirements
    - Minimum of 12 characters

        - Cannot be the same as your user ID or previous six passwords
        - At least one upper case letter
        - At least one lower case letter
        - At least one numeral OR one symbol
        - Must be changed at least every 365 days
    - Next steps
        - Beginning Sept. 30, 2021, existing passwords will be set to expire following the schedule. New passwords will need to meet the new requirements.
        - Account last name begins with:
            - A - G: Sept. 30
            - H - M: Oct. 31
            - N - Z: Nov. 30
        - To avoid this forced reset, you can change your password now using the information on the following page: https://ou.edu/ouit/password.
    - Can no longer use passphrase
        - This is more universal for all campuses
- Multi-factor authentication changes - Aaron Baillio
    - Nothing will happen with faculty, staff, students this year
    - IT will start testing internally with Office 365 and other minor systems in September
    - There is a new app from PING (our SSO provider) to replace Duo
        - Advantages
            - Dynamic sign-in process
            - Makes it more seamless
            - A lot in cost savings
    - Will start marketing broadly in the Spring
    - MFA rolling out to more services
        - There is a group looking are more places to role MFA out to
        - Almost all remote access will have MFA requirements
        - Andy Fagg - Is MFA being attacked?
            - Aaron Baillio
                - Nothing is infallible
                - It's a cat and mouse game

    - It's a level of risk we are will to carry
    - Ping has a better track record than DUO
    - It's a NIST recommendation

IT Policy Updates - Nick Key

- Reminder of the Cyber Security policy was pass earlier this year
    - Goes into effect January 1 for all distributed IT
- End-user Device policy
    - Approved 1 month ago
- Coming up next is Data Backup and Retention policy
    - Not shared yet for feedback
    - April Dickson will let us know
- Remote Access policy on deck after Data Backup and Retention
    - Probably will require MFA
    - Consolidate SSH bastion hosts
    - Document SSH gateways
    - Andy Fagg - This will affect external data collection
    - Policy will need to adjust to the use cases
    - David Horton - We need a good inventory of these hosts and good firewall policies

Privacy - Andy Fagg

- Logging browser history
    - Twitter post from staff member about memo indicating that browser history is being logged
    - Nick Key, Aaron Baillio, David Horton
        - IT does track network activity
        - Big picture is that information is scanned
            - IT has a lot of protected data
            - Data that is collected has to be protected
            - Logs are classified appropriately and controls are in place
        - Logging started years ago with Carbon Black
        - IT does log all DNS requests

        - Can be correlate with other logs to track down end user
        - If your device is reaching out to bad actor DNS, IT needs to look at other malicious activity with that device
        - Logs retained for 90 days
    - IT is not picking a faculty and looking at their activity
        - With 45,000 users we are just using the technology to flag suspicious activity
    - CrowdStrike has replaced Carbon Black. It's not logging DNS, just very specific process activity.
    - IT has been doing scanning network activity for years. Tools are better now.
        - IT has to retain the logs for a certain time according to policy (90 days)
        - All security staff have taking training and signed NDAs
        - All log backups are encrypted and put in a safe place
        - IT is scanning anything through the firewall
            - Cannot see individual packets if the connection is encrypted, but can see connections
    - Office of Legal Council has a process to request this log data. There are a lot of safeguards in place to access this data.

Future Meetings

- Projects for new year?
    - Policy and standards - Andy Fagg
        - Andy Fagg - Concerned they are written from a legal perspective. Hard to read by end users.
            - Creative Common licenses. Make it readable by humans. Parallel languages. It would be helpful if we have this for our policies and standards.
        - David Horton - The only people that asked us for the policies are auditors. That's why they are written that way. That doesn't negate what you are saying. Maybe we can put a cover sheet "what does this mean to you".
            - There is a course on Cyber Security policy course on HR website
            - Departments needs to hold IT (central and distributed) responsible for help
            - IT professionals have to understand this information.
            - If you support an information system, you are subject to all policies. You have to understand and support the policies.
    - IT governance framework - Nick Key

        - Close to complete with implementation
        - Working on finalizing committee membership
        - We really want to plug into existing committees
        - Goal is to each out to Faculty Senate to fill spots
        - Andy Fagg - Is there a relationship between ITC and framework?
            - Nick Key- Yes. This is truly system level. We need to get independent guidance aligned.
                - Support goals for efficient and prioritization
        - David Horton:
            - Governance is alway evolving
            - New tool called Policy Tech
            - IT will be plugging policies into Policy Tech tool to publish
            - There is a lot of interest in IT risk at the Regents
    - Data sharing - Andy Fagg
        - I share data with HSC via encrypted disks
            - Would like to do this over shared network drives
            - Including HIPPA data with other institutions
                - Can use trust contracts with third parties?
            - Aaron Baillio:
                - Jill Raines has approved Office 365 for HIPAA data
                - Working with Dr. Neeman and April with research and HIPAA data. Comes online at the beginning of 2022
                - Also working on ways to share more sensitive data than HIPAA
    - David Horton - All good topics to discuss for the next year.
- Meeting times - Andy Fagg
    - Meetings (almost) every 3rd Monday:
        - Sept 20, Oct 18, Nov 15, Dec 13 (exception), Jan 24 (exception), Feb 21, Mar 21, Apr 18
    - Meeting time: Stick with 8:30 am or try for later?
        - Committee: 8:30 am on Monday is fine
    - Still waiting on new appointments from faculty senate

Meeting end: 9:25