Group: Information Technology Council 2021-2022
Subject: Minutes for the ITC Monthly Meeting
Date: Monday, December 13th, 2021, 9:00-10:00am
Location: Zoom

Recorder: Aaron Biggs
Attendees: Andy Fagg (Computer Science), Aaron Biggs (Provost Office), Nick Key (IT), Ross Mehl (Extended Campus), Jenel Cavazos (Psychology), Richard Sprecker (Drama), Eric Zemke (Libraries), April Dickson (IT), Char Eby (Computer Science), David Horton (IT), Konstantinos Karathanasis (Music), Rin Ferraro (Graduate Student Senate), Daniel Deering (VPR)

**Review of November Minutes: Andy Fagg**

Passed

**Computer Standardization: Nick Key**

- We have compensating controls in place for M1 Macs now. When the user logs in for the first time, the computer is automatically registered with the JAMF server. Will kickoff CrowdStrike and Endpoint Protector installs.
- CrowdStrike is next-gen antivirus
- Endpoint Protector manages the encryption of removable media. Equivalent to Dell Encryption Suite.
- We can still make exceptions if needed through the standard exception process.
- To initiate this process, the actual user needs to log in, not the IT person.
- We are delivering the M1 Macs now.

**Endpoint Management and Device Support - David Horton, Nick Key**

- Konstantinos Karathanasis: When the new M1 Macs were delivered, some of our faculty got a message about JAMF enrollment and freaked out about constantly being monitored. Also, can IT just shut down the computers remotely?
- Nick Key: All web activity is monitored all the time. This network-based monitoring has been done for years. IT logging is focused on network traffic. We are not interested in what websites individuals are going to. We will shut machines down if they pose a threat to the network. We will call you and talk to you before shutting down the computer's access to the network. We will not leave you hanging.
- April Dickson: We will always try to find the admin for that device if possible first before shutting down access to the network.
- Nick Key: Any logging or monitoring we are doing is automated just to protect the network. IT personnel are not looking at access logs (except when flagged as suspicious from a security perspective).
- Shutting down network access mostly happens in dorm rooms.

- Eric Zemke: OU Libraries has been in contact with IT about possible compromised computers. So far a non-issue.
- Would it be possible to have a basic knowledge base for distributed IT so we can say what CrowdStrike does, this is how you will be monitored, this is how IT will escalate issues.
- Nick Key: Just think about the amount of data that is generated at OU. We have a security team of 19 people. They just don't have the time to personally monitor data. We have to automate it. We are only worried about attack vectors.
- Eric Zemke: Who do we need to contact about associating new M1 Macs to the OU Library JAMF server instead of new central JAMF server?
- Nick Key: M1 Macs have to be on the central JAMF server. You need them to be associated with the OU Library JAMF server, you'll need to submit an exception for review. We are 12 months out from pushing everyone to the central JAMF server anyway. Which will help with notifications as well. Let's discuss what the transition will look like with April, Millard, and myself.
- Andy Fagg: What is JAMF?
- Nick Key: JAMF is basically an endpoint container. Puts computers in appropriate groups. With the groups, we create policies, patch management, define what software is automatically installed, easy deployment of images, reporting (how many have AV install, etc…), etc…
- Andy Fagg - Define "network joining".
- Nick Key: In the long term, every computer on campus needs to be on the Active Directory domain for authentication or there needs to be a security exception in place.
- April Dickson: Local authentication - If your computer is domain joined, you can still authenticate without a network access. You don't lose local access (at least on Windows).
- IT acknowledges that faculty need admin access and the ability to install software
- Konstantinos Karathanasis: can you send us the link for exceptions. Echo Eric's comments to reach out to faculty to communicate on this process. Need to decrease people's fears.
- Link to exemption form - https://itsupport.ou.edu/TDClient/35/Norman/Requests/ServiceDet?ID=171&SIDs=1563
- Nick Key: The Regents have been very clear on the endpoint management. We are going to do everything we can for the research. Mobile weather data capture is an example. They need computers with no AV that can slow down capture. This is an easy exception. We just need a clear boundary for these exceptions. We are 5 - 7 years behind the industry. This is top of mind for the Regents.
- David Horton: We are increasing our governance with faculty representation. Have committees help us with exceptions.
- Nick Key: Teaching and Learning Technologies Advisor Committee (TLTAC) co-chaired by Aaron Biggs and Valerie Williams is example of such a committee.
- Eric Zemke: I don't' think we have a question about how or why, but we need a document for the what.
- Nick Key: We are not quite there yet. We need to get through hires. We have the tools, but not the processes in place yet.

- We are presenting to Faculty Senate this afternoon.
- Andy Fagg: What about personally owned machines?
- April Dickson - If you are using a personal device for OU business, it will need to meet our controls. Not looking to install OU controls on those machines. You'll need to use a VDI (Virtual Desktop Interface) for the most sensitive data. We are going to ask that they use AV, password, and enable encryption. Same containment rules (network block) apply for compromised personal devices. IT will try to contact the person if possible.
- Individuals can be financially liable for breaches if they are using their own machines for university business.
- David Horton: We've had the capability to block network access in place for years with Net-Reg.
- Andy Fagg: What about student devices?
- April Dickson: General best practices. No policy for students right now.
- Nick Key: Student employees working on personal devices for OU Business will operate much like OU employees. Same rules apply.
- When individuals use personal machines, they are taking on potential financial liability.
- Andy Fagg: What happens when an issue is detected with a personal device?
- April Dickson: We can't shutdown personal devices. For systems that are managed, we'll investigate and contract. If all else fails, we'll disconnect from the network. We won't shutdown (OU managed) computers unless it's a major issue like ransomware.
- David Horton: Asset management is designed to allow us to contact quickly.
- Andy Fagg: How do we know it's IT when they call?
- April Dickson: We won't call directly. We'll use email until we establish alternate contact mechanism.
- Aaron Baillio: With Net-Reg registration, we know who the device is registered to.

**BitLocker incident**

- BitLocker: central escrow key system for encryption of devices
- These incidents add to anxiety about the new mechanisms being put in place
- David Horton: There was an issue with BitLocker. We have 10,000 devices registered. We think the issue involved timing and sync of some patches. About 950 of the machines were affected. We were able to get the keys back out to the users so they could unlock their devices. So that was working as intended. Primarily impacting HSC.
- Part of the challenge is that if we managed these endpoints, we could better sync devices and server solutions.
- We are also looking at moving away from Dell Encryption.
- Andy Fagg: Centrally managed keys?
- David Horton/April Dickson - Reports that the device is encrypted. Encryption itself is good, but the computer has to report in that it was encrypted.
- Safe harbor: If we can show that the device was encrypted at time of loss, the investigation usually ends. We don't have to do notification, financial penalty, etc…
- Andy Fagg: Why not one and done for encryption?
- David Horton: We may need the ability to decrypt if needed and we also need to show that the device was encrypted at the time of loss.

**Preferred Names in the OU Systems: Nick Key**

- Nick Key - Automation of Preferred name changes will be in Banner/Canvas after the break. Always new tools that need to be addressed. If you run across a tool that is not the using preferred name, let us know.

**Authentication: Nick Key**

- Andy Fagg: I finally received the email to change my password. Seems to be on the normal schedule.
- Nick Key - We started with students and are working in increments. Needed to space out password renewals. Better for support. Just beginning faculty and staff now. You might have to change twice if you hit the normal schedule now and your new schedule is coming up after break.

**UNICEF Spam Status: Andy Fagg**

- Andy Fagg: We are getting a lot of these UNICEF spam emails. I've been reporting them as phishing. Told it was not phishing, but spam so deal with it.
- Char Eby: IT lectures us about spam vs phishing. Not a good experience.
- Nick Key: Can you forward me that email?
- Staff are being referred to training for unknown reasons.
- Phishing training can get annoying. Training is difficult. 14-15% of people still enter credentials. This is the most effective and best practice way to train.
- Aaron Baillio: Phishing email should go out once a month.
- Please contact me directly to look into the phishing training emails.

**End of meeting: 10:00AM**