**IT Gov Minutes**

October 5 & 19, 2022

Via Zoom

**Attendees:** Brenton DeBoef (absent 10/19), Melissa Frost, Brandon Fuller, Marta Gomez-Chiarri (absent both), Michael Greenfield, Joshua Gyllinsky (absent both), Amanda Izenstark, Shaun Kavanagh (absent 10/19), Karlis Kaugars, Michael Khalfayan, Kara Larsen (absent 10/5), Ian Lester, Dean Libutti (absent 10/19), Matt McDonald (absent 10/19), Ryan Menard (absent both), Sanjay Kumar Mupparapu, John Stringer (absent 10/19), Kathleen Torrens (absent 10/19), Ted Walls (absent 10/19)

**Guest:** Heath Loder (10/5)

1. Approval of Minutes
   1. June 2022
   2. Ian moved to approve minutes as presented.
   3. All present voted to approve.
2. CIO Updates
   1. Ted is now chair of Fac Sen Committee on IT & Infrastructure
   2. Amanda is now Library Rep
   3. Matt McDonald is rep from Communications, Marketing & External Communications
   4. Shaun is replacing Lori C while she’s on her ACE fellowship
3. Project Status Updates
   * 1. Biggest change is that we’re pursuing an E-procurement system so Workday blueprinting project being postponed (also due to funding questions with the Legislature)
   1. No other questions or comments from the group
4. Desktop Support Update (Heath Loder)
   1. Founding manager of Endpoint Support Services
   2. Primary goals to meet compliance standards required to get cyber insurance
      1. Unique digital identities
      2. Patch management, anti-malware, monitoring
      3. At-rest encryption (BitLocker, FileVault)
      4. IT approved software only
      5. Remote work
   3. Timeline/Progress
      1. June 7, 2022, Endpoint Protection Policy
      2. August 15 endpoint support position created
      3. October 5 compliance with Multicultural Student Services, Pharmacy, Ranger, Tyler VR Lab, and CEPS in progress
   4. Challenges & Solutions
      1. Active Directory access / use
      2. Distributed IT access
      3. Name-based licensing
      4. PeopleSoft Financial/HR test page
   5. Roadmap
      1. Limited access to Jamf/Intune to distributed staff and train
      2. Additional “Train the Trainer” training sessions
      3. Remote Access/Administration (UAC)
      4. Apple School Manager/Automatic Device Enrollment
      5. Intune/Jamf/Microsoft Endpoint Manager Integration
      6. Compliance Reporting (Intune)
   6. Approach
      1. Bring into compliance with PII (HR, Admin & Finance, Payroll)
      2. Public machines (labs, kiosks, GAC computers, etc.)
      3. Faculty/Staff on-premise machines (no PII)
      4. Faculty/Staff remote machines
      5. BYOD
   7. Questions?
      1. Brenton: ITS vetting machines that are used for research purposes where software development is being used and includes hacking it to do new things – will these groups be okay with having your approval? Karlis: Gaurav is leading this charge working with faculty who will need administrative access and those faculty who will do other modified activities. We are deploying a research DMZ and it’s being led by Gaurav as well. These machines will not be allowed to access sensitive university data and programs.
      2. Matt: what’s in place to tighten the timeframe for downloading programs and what is the anticipated process for BYOD? Heath: installation of software is a tiered approach and a balance between security and usability. Before we strip away end-user admin rights, we need all the other pieces in place as previously mentioned.
      3. Sensitive data on a machine needs to be locked down and separate from research machines in a DMZ that cannot have any PII. Research machines do need to be protected so the research data isn’t stolen as it’s very valuable information.
      4. John: his area has software packages that are not on the approved list so how do we get them in the queue for approval? Heath: there is no approach yet and he will begin addressing this immediately. We need to set a prioritization list.
      5. Ian: what about printers, webcams, speakers, etc. that all require driver installation which is software.
      6. Matt: can we look to our peers so we can learn from their processes? Karlis: yes, there’s a thread of Educause in active discussion with about 50 CIOs with elements we’ve previously covered.
5. Security Environment at URI (Karlis Kaugars)
   1. Infrastructure needs adequately protected by MFA to administrative access to servers and systems. In pretty good shape right now.
      1. Network components (firewalls, routers, etc.) should be complete within the month.
      2. Servers into protected environments that can be accessed only by a jump server.
      3. Backup DR in pretty good shape (98% of servers being replicated into AWS) and tested on prem restoration of these and it’s been successful. However, if both Tyler and Warwick go done simultaneously, we have not met with success in restoring them to the cloud and Chi continues work on it.
      4. We have not met with success with everything, Oracle cloud to servers’ restoration with PS Financials did not go well but work continues.
   2. Services delivery in reasonable shape due to SSO with MFA and are largely in compliance with policies.
      1. Great concern with pocket systems out there and having them in compliance by January.
      2. Not great access to these and unsure of progress – it’s a serious worry.
      3. Penetration with distributed tech areas is hit or miss. Hoping that by continuing the conversations we can make some progress.
      4. Weighing in with Executive Council for enforcement of compliance with sanctions.
   3. Questions?
      1. Kara: auditors presentation mentioned the need for policies, what does Karlis feel are the gaps as we’ve just put in three very strong and encompassing ITS policies. The auditors were using policy in a different way – for an ITS procedural documentation. Mike K is working on this with an ETA document; it’s in review phase and then to the edits.
6. Proposed Projects: Smart Sheets and Byte Technology Smart Fridges (Shaun Kavanagh)
   1. Postponed until November meeting when Shaun is available.
7. New GLBA Security Requirements: What It Is, Importance & What Needs to be Done (Michael Khalfayan)
   1. URI needs to comply with several regulations (HIPPA, FERPA, PCI (payment card industry – how you can collect and process cards) compliance, GLBA (law passed by Congress applicable to include Department of Ed because we process financial information of parents & students) compliance) and the work is in process with the last two.
      1. Working with consultant for what we need, what is missing, and reviewing this on Friday on PCI and may do the same process with GLBA.
      2. They are both security best practices.
      3. FTC enforces compliance with GLBA, and URI must be compliant by December 2022 or face fines.
      4. Services covered: student loans, bank loans, applications, billing information, tax return information, DOB, payroll, W-2, etc. – covers all financial information related to faculty, staff, and students.
      5. Privacy rule and safeguard rules are the main objectives to protect that information.
   2. These entities are informing URI of what we need to do for cyber security, and we are responsible for compliance with the rules.
      1. Will do a gap analysis to see what we are missing across the university, university systems on premise and in the cloud.
   3. The library no longer collects fines except for late laptop returns.
   4. Research will be subject to these rules with their new software.
   5. ISORA will allow us to conduct surveys with all departments to gather this needed information.
   6. Questions? None
8. Open Forum
   1. Mike K
      1. Security Awareness Training is doing a reboot as it relates to part time faculty union rules. Thank you to Ted, Amanda, and Rita for the information we needed and assisting with the messaging to be certain it was clear and accurate. Look for a new message for SAT to come out soon.
   2. Brandon
      1. Update on Google on data caps, storage, etc.? No changes right now. Experiencing difficulties getting a contract with Google right now. Had planned on and budgeted for based on contract Google has with Internet 2 (that negotiates on behalf of the entire membership which allows for extraordinary good terms). Purchasing refused this path and insists that it goes out to bid even though Internet 2 will not bid as they choose to not be compliant with State of RI purchasing laws. We will push through the system again, as we did with ServiceNow which ran up against the same issue and the State of RI allowed us to purchase through Internet 2 because it saved so much money. All this means, we do not have full access to all the Google tools and won’t by January.
   3. Upcoming Meetings
      1. Next meeting is WED 11/2/2022 at 9 AM via Zoom.