LSU

Faculty Senate

Ad Hoc Faculty Senate IT Committee Meeting

12 May 2023

11:00 AM, 1008B Center for Computation and Technology

Minutes of the Meeting

I. **Call to Order** by Singh at 11am

II. **Roll Call**

Present: Param Singh (Chair), Gerry Knapp, Ken Lopata, Samuel Robison, Larry Smolinsky, Craig Woolley (Ex-Officio), Sumit Jain (Ex-Officio), Scott Baldridge (special advisor)

John Buzbee (The Reveille)

Absent: Juana Moreno, Fabio Del Piero, Fanny Ramirez, Jeffrey Roland

III. **Public Comments**: There were 3 public comments.

- Kevin Ringelman (School of Renewable Natural Resources, LSU and LSU AgCenter) commented that ITS must make these policies available for viewing by AgCenter-majority employees who are blocked from accessing them on Box. It is not appropriate to put that responsibility of sharing them to an unnamed "administrator" in the AgCenter.
- Daniel Tirone (Department of Political Science, College of Humanities and Social Sciences) emphasized the role of shared governance in the process of revision of IT policies. Expressed concern about ITS' proposed statement on consequences of violation and referring employees to a disciplinary action. If such a statement is included, then the entire process must be completely transparent, and faculty should be involved to oversee the process. The threat to tenure does not only come from outside the university but also from inside if transparent processes and shared governance are not in place.
- Ilya Vekhter (Department of Physics & Astronomy, College of Science) mentioned that he worked at a national lab involving nuclear secrets and the rules were milder than the ones ITS is imposing. The intrusive obsession with security at any cost and threats of termination reminded him of his Soviet childhood. The university leadership needs to decide whether IT exists to support the core mission of an R1 research university or to be a detriment in that mission.

IV. **Approval of minutes from ad hoc FS IT committee meeting on 5/10/23:** Knapp moved to approve. Smolinsky seconded. Passed unanimously.

V. **Chair's updates:** CIO Woolley sent a statement on consequences of policy violations which was shared with some faculty members after his permission. In the ad hoc FS IT meeting of May 10, some committee members asked ITS to provide a draft procedure which will handle non-compliance and infractions. In particular, they were concerned whether minor infractions would result in a disciplinary action. A draft statement has been proposed by ITS which is a topic of discussion in New Business.

The feedback received was all against inclusion of any statement referring to PS104 or disciplinary action. Comments from two faculty members stated:

- "I have been at two national laboratories, one as senior research the other in an upper management position. Both laboratories were involved with national security working involving Q-clearances. Neither had policies like the ones proposed. The way we would go about developing policies is to first understand how the organization operates to do its core business and mission, then develop policies and infrastructure to ensure the changes don't impact the organization's ability to do its work. I don't see this in these documents. It seems IT is developing policies that are contrary to the organization's work environment."
- "More importantly, the reference to PS-104 is unacceptable. Full stop. PS-104 covers dismissal of faculty, including tenured faculty, for cause. I fail to see how a wide range of cases that might lead to an "egregious violation" as defined could be grounds for termination for cause. The vast majority of faculty have contractual obligations to teach and conduct research; some additionally have contractual obligations for some small amount of service. (Most do service even though it's not in their contract.) Precious few of us have IT or cybersecurity responsibilities in our contracts. If a faculty member makes an innocent mistake that leads to a complete collapse of the network (say), how can that be cause for termination? We haven't been negligent in our duties; we've made a mistake. This might be fixed by specifying that the violation be malicious or with malicious intent. But even then, we should be *__very__* careful about writing referral for PS-104 proceedings into anything."

Other comments on ITS are also being received which are overwhelmingly critical of the current state of these policies. Two of the faculty members stated:

- "In looking over the various ITS proposed Policy Statements, it seems that one thing that is missing is what happens when an exception happens which is not catered for in the Policy Statement. It would need to be dealt with by someone or some group. Who would be responsible for handling exceptions? This is not spelled out in the policy statement and needs to be. And following on from this, there should be appeals process for the individual or group who brings up the exception but feels it has not be dealt with appropriately."
- "The overarching concern I have regarding the proposed "LSU IT Policies" is not with the "LSU IT Policies" themselves, but rather with "LSU's IT Staff's" implementation of those policies as it relates to data generation and/or management, preservation, and retention of the same, all of which directly impacts LSU's research-active community that rely heavily on the use of "IT Resources" within and even more importantly beyond those provided by LSU itself. Specifically, LSU's research community seems to have lost its long-standing role on

> being able to check-point LSU's IT-Staff 's interpretation of what it needs to do to ensure that the implementation of "LSU IT Policies" is in accord with LSU's IT Staff's interpretation of the latter, with little to no regardless of the impact this may have on the LSU's research community. Researchers understand that what transpires on the local level within LSU itself is LSU's business, but the implementation of "local regulations" can run afoul of "global expectations" of LSU's research-intensive programs, especially those involving the sharing of data among diverse research "teams" outside of LSU itself; specifically with research collaborators from other LSU-like institutions (national and international) and also as this extends to government-managed laboratories and complementary business-sector entities, not infrequently beyond even our own national boundaries."

Singh emphasized the need for a transparent process involving Department Chairs and Deans if ITS wishes to include any mention of disciplinary action in the policies.

Lopata moved a motion to suspend the rules and consider the new business before the unfinished business. Knapp seconded. Passed unanimously.

VI. New Business

- ITS' proposal to add wording on consequences of violation of IT policies only in PS-120: "Violations of any policies and standards may result in blocking of network access of IT asset(s) and/or user(s). Any egregious violation, i.e., violations resulting in a security incident classified as Critical or High, as determined per Security Incident Response (please refer PS-133-ST-2), would be referred to the following for disciplinary action:
  a. LSU HR as per university policy PS-08, or
  b. Office of Academic Affairs as per university policy PS-104, or
  c. Office of Student Advocacy and Accountability as per Code of Student Conduct."

    - In the meeting of May 10, some committee members asked ITS to provide a draft procedure which will handle non-compliance and infractions. Woolley mentioned that the proposed language was an initial draft to receive feedback from the committee and potentially others to see if it addressed the concerns raised and if not, what modifications would need to be made. It had inputs from HR and General Counsel and ITS would consider any revision to the proposed statement. Singh expressed concerns that HR and General Counsel agreed to this proposal when there is no standard which clearly defines what is Critical or High Risk. Smolinsky emphasized that IT policies can not refer to PS104 or any such policy. It is neither in domain of this committee nor of ITS to frame policies referring to disciplinary action. Lopata mentioned that ITS must not play the role of a cop. Knapp emphasized that any violation of policies can in principle lead to termination. Jain provided examples of security incidents which may or may not come under egregious violations. Baldridge recommended to change violation to non-compliance.
    - Lopata moved to change the proposed statement to "Non-compliance with any IT Security Policies and Standards may result in blocking of network access of IT asset(s) and/or user(s) until the identified issue(s) has been resolved in collaboration with appropriate support personnel and/or user, where applicable." Seconded by Smolinsky. Passed unanimously.
    - Above statement added to PS-120 as a new section E.

VI. Unfinished Business

- Discussion on IT Policy PS-121

1. PS-121-ST2 (B2): Discussion on encryption led by Lopata. Statement modified from "All end user computing devices must be encrypted in a manner consistent with the data stored on them and as outlined in the Encryption Standard (PS-126-ST-1)" to "All University owned end user computing devices must be encrypted in a manner consistent with the data stored on them and as outline din the Encryption Standard (PS-126-ST-1)."

2. PS-121-ST-2 (B3): Lopata, Robison and Jain discussed about various approved devices physically and in cloud. Statement modified from "Users must store all sensitive/confidential University data on authorized and approved storage services, whether on premise or cloud." to "Users must store all sensitive/confidential digital University data on University authorized and approved storage services, whether on premise or cloud. Please refer Appendix A in PS-124-ST-2 Data Handling standard."

3. Singh requested that standards which are getting revised should be available for view to TSPs. Also requested that the staff senate should be reminded to share the files with staff. Lopata and Robison shared this concern.

4. Discussion on BYOD led by Knapp, Robison and Jain. PS-121-ST2 (D1a) changed from "Devices must have the latest firmware updates, patches, service packs, and/or operating system version." to "Devices must have the latest and/or supported firmware updates, patches, service packs, and/or operating system version."

5. PS-121-ST2 (D1c) changed from "BYOD devices must not be configured in a manner to bypass security measures put in place by the manufacturer (e.g., jailbreaking)." to "BYOD devices should not be configured in a manner that increases the risk to the University's environment. Where a device configuration is modified, e.g., jailbreaking a device, appropriate measures must be taken to minimize risk."

6. Discussion on endpoint protection led by Lopata, Jain and Baldridge. PS-121-ST2 (D1d) changed from "BYOD devices must have endpoint protection, anti-virus, and/or anti-malware application installed, configured, operational, and be up to date." to "Where feasible and available, BYOD devices must have endpoint protection, anti-virus, and/or anti-malware application installed, configured, operational, and be up to date.

7. Discussion on usage activity in PS-121-ST2(E) led by Knapp, Lopata, Jain and Smolinsky.

Robison moved to postpone the remaining items to the next meeting. Knapp seconded. Passed unanimously.

Adjourned: 12:38 pm.

*It is intended that public comments may be made (1) when they relate to a matter on the agenda and (2) when individuals desiring to make public comments have registered at least one hour prior to the meeting by emailing psingh@lsu.edu. When registering, individuals should identify themselves; the group they are representing, if appropriate; and the topic on which they would like to comment. To ensure that the meeting is conducted in an efficient manner, each individual will be limited to 3 minutes for their public comments and the Chair reserves the right to limit the total number of public comments if necessary.

The LSU Faculty Committees may meet in executive session as authorized by La. R.S. 42:17.