Ad Hoc Faculty Senate IT Committee Meeting

7 June 2023
11:00 AM, 1008B Center for Computation and Technology

Minutes of the Meeting

I. Call to Order: Singh called meeting to order at 11:00 am

II. Roll Call

> **Present:** Param Singh (Chair), Gerry Knapp, Juana Moreno, Sam Robison, Craig Woolley (Ex-officio), Sumit Jain (Ex-officio), Scott Baldridge (special advisor)

> **Absent:** Ken Lopata

III. Public Comments: None

IV. Ad Hoc FS IT Meeting Minutes Approval from 5 June 2023: Moreno moved to approve minutes. Passed by majority vote. Robison abstained.

V. Chair's Updates: None

VI. Unfinished Business

- Discussion on IT Policy PS-126
    - Singh shared feedback received on PS-126 with detailed comments and suggested edits.
    - Discussion about limitations with full disk encryption for certain systems including Linux based and dual boot systems. Baldridge and Singh recommended to change PS-126-ST1 A1 to include a note: "NOTE: If whole disk encryption is not feasible due to hardware and/or technical limitations, appropriate compensating controls must be implemented to secure any private and/or confidential data stored on such endpoints. Users that are unable to do whole disk encryption can work with LSU IT Security and Policy Team (ITSP) to determine compensating controls."
    - Knapp recommended adding the caveat of "Wherever encryption is used" in points 2, 3 and 4 of PS-126.
    - Baldridge and Knapp asked to revise the definition of encryption to correct the issue of reversibility as follows:
    "Encryption – Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. The corresponding reversal process is called "decryption", which is transformation that restores encrypted data to its original state."

- Discussion on availability of recovery keys for all users. Jain mentioned that ITS expects a self-service solution for all University owned Windows machines which are on LSU domain in a time span of 1 year. Till then TSPs will have easy access to these keys. Singh requested that there should be a GROK article on this to guide faculty, staff and students.
- Robison and Moreno noted that complying with encryption policies at a university wide level would require adequate training of concerned department personnel. Jain mentioned that there are about 9000 Windows machines that are part of the LSU domain of which about 5000 have encryption via BitLocker managed through SCCM.
- Jain mentioned that there will be GROK articles and a Moodle course to educate users on IT policies.
- Robison mentioned that there can be instances where exemptions are needed on PS-121-ST1(A2) to obtain the data. Mentioned cases where Federal agencies do not allow data to be encrypted. Jain mentioned that in such a case ITS would work with faculty to allow any exceptions.
- In PS-121-ST1(A2) "system" was replaced with "servers, storage systems" and examples were added for portable/removable media.
- In PS-121-ST1 (B1) the term "over the network" was added to add clarification for transmission of data. A reference to PS-124-ST2 was added.
- Discussion on most points in section B of PS-121-ST1 to be relevant only for system administrators and being too technical. As a result, (B2) was moved to (B6) and a note was added to the end of Section B – "NOTE: Points 4 through 7 would generally be met by system and/or application administrators and should not impact users."
- Discussion on whether encrypted files can be sent using insecure methods. Jain replied that in general this is becoming quite difficult to achieve.
- Discussion on examples to be added to PS-124-ST1 (B4), and what is meant by affiliated. Changed to "LSUAM and affiliated websites (e.g., LSU website, myLSU portal, Workday, etc.) and web-based applications must be served via HTTPS (TLS 1.2 or greater) regardless of data classification."
- Discussion on Section C being too technical. Its heading now included "(for system and application administrators)"
- Singh expressed concerns that PS-121-ST1 (C1) does not allow compliance even at present stage or in near future for LSU. Gave example of OpenSSL which is only expected to be compliant with FIPS 140-3 in late 2024. As a result, FIPS 140-3 was replaced with FIPS 140-2 and a note was added – "NOTE: New development or implementation should use FIPS 140-3, where feasible."
- In PS-121-ST1 (C2) specific key lengths were removed, and the statement was rephrased as – "The following symmetric algorithms with the recommended and supported key lengths…"
- In PS-121-ST1 (C5) clarification was added that the statement relates to "for sites associated with the University".

The Meeting was adjourned at 1:01 pm.