Ad Hoc Faculty Senate IT Committee Meeting

23 August 2023
9:00 AM, 1008B Center for Computation and Technology

Minutes of the Meeting

I. Call to Order: Singh called meeting to order at 9:00 am

II. Roll Call

Present: Param Singh (Chair), Gerry Knapp (Secretary), Ken Lopata, Juana Moreno, Sam Robison, Larry Smolinsky, Craig Woolley (Ex-officio), Sumit Jain (Ex-officio)

Absent: Scott Baldridge

III. Public Comments: None

IV. Ad Hoc FS IT Meeting Minutes Approval from 9 June 2023: No amendments proposed. Moreno moved to approve the minutes. Passed unanimously.

V. Chair's Updates: Singh did not have any updates. He thanked the committee for its service.

VII. New Business

1. Summary of revisions in PS120, PS121, PS124 and PS 126.
   - Jain prepared and went over a summary of the changes recommended by this committee in the spring and early summer. See Addendum 1 to minutes below for the summary. Jain confirmed that all recommended changes were accepted by the governance committee and academic affairs.
   - Moreno requested that it would be useful for the committee to see example baselines before end of current review cycle; Jain indicates they are currently working on the baselines, so should be possible.
   - Lopata noted our committee's name is embedded in the standards, and the name may change (e.g., removal of ad hoc); Jain indicated the name change can be done easily, no formal approval will be needed.
   - PS-121-ST-2: Lopata and Moreno raised concerns on whether any usage activity is *not* logged/written – for instance, can admins read user emails without a documentation trail? Jain noted this is handled in procedures rather than standards, and that all such activity can only be done in response to written requests from specified units (e.g., HR, LSU police). Lopata asked about whether there was always documentation for ITS activities in response to security events or other incidents. Jain indicated that generally there is documentation, but regardless all activities are logged in activity logs of the various systems (e.g., last 30 days for any query on Microsoft email; 180 days where admin looking at email content (requiring e-discovery – a formal documented process) – and only 2 people on campus have permission to do this); Lopata and Singh asked whether users can request logs of who has accessed their email or other resources? Jain indicates that yes, they can.

- Jain notes that data governance related sections may require modification as Dr. Arbuthnot (new LSU Chief Data Officer) is currently reviewing and refining data management processes and governance framework; Singh asked if she is aware of the review our committee is doing; Jain indicates she is, and that any proposed changes from the CDO will come through the ad hoc FSIT committee for review.
- Singh noted that 89 numbers are an important issue to faculty. Woolley and Jain noted Dr. Arbuthnot seems to agree with this. They suggest meeting with her to discuss (perhaps through FSEC rather than this committee).
- Moreno asked about the timeframe for replacement of the mainframe systems. Jain and Woolley indicated about 1 year for Workday Student, sometime in 2025 for IAM (identity and access management) replacement. 89 numbers will not be an identifier in the Workday system as this is an LSU system-wide implementation. Moreno reiterated discussion needed now so can address 89 number issue in these implementations.
- PS-124-ST-2 Section D, point 3: Robison noted that may need to add language on legal agreements in research data sharing across organizations. Jain will review and see if a change is needed or if addressed elsewhere.
- Lopata noted it will be helpful to have an index and maybe just a single page brochure of key points for faculty on these policies and standards; Jain noted they are working on an index (as a GROK article) and a Moodle training course (will be optional) with training videos relating to each of the policy statements. The committee was concerned with these being published prior to completion of our initial review of all the PS and standards Woolley and Jain indicated they supported development of a key points brochure.
    - Motion made by Knapp and passed unanimously to request putting a hold on publishing videos until first round review is over. Woolley and Jain agreed. They will also provide the committee with access to review the videos before they are published.
    - Motion made by Robison and passed unanimously to identify key points for the one-page brochure. Lopata and Woolley will collaborate to identify key points for the brochure for discussion in an upcoming meeting.
    - Jain noted that the PS and standards would be constantly undergoing revision. Knapp asked that ITS consider sending out periodic updates to faculty and staff summarizing "recent changes".
- Singh and Moreno asked that it be noted in the index which PS and standards were still under review by this committee; Knapp asked that the training videos indicate last revision date. Woolley and Jain agreed.
- Robison asked about the timeline for approval of any changes recommended by the committee this semester. Jain indicated weeks to months, but may be into next semester for changes required additional administration review.

Announcement: Moreno will need to leave at 10:15am for future meetings. Was agreed to move future meetings to 8:45-10:15am on each Wednesday of the Fall 2023 semester.

The Meeting was adjourned at 10:31 am.

Addendum 1
Summary of Spring/Summer Policy and Standard Changes

PS-120

Policy Statement

- Added definitions for Incident, Incident Response, and IT Asset.
- Added examples for Data Functional Owner, Data Steward, and Data Custodian (A.1)
- Added the following in D.3. for Policy Management:
    - "LSUAM must define an exceptions process for all policies and standards including appeals process for exceptions that are denied."
- Added Section E titled "Policy and Standard Non-compliance"
    - "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."

PS-120-ST-1

- Added additional context to the role of Data Functional Owner:
    - "As it relates to research data, the functional owner would be appointed by unit head, department chair, or Office of Research and Economic Development; where appropriate, the Principal Investigator (PI) or lead researcher should serve as the Data Functional Owner. As it relates to instructional materials, where appropriate, the Data Functional Owner should be the creator of the materials. Data Functional Owners are not necessarily the owner or intellectual property owner of the data."
- In Section K related to Data Consumer point 4 was updated as below (changes underlined):
    - "Maintain adequate operational controls to ensure data protection <u>as instructed or defined by Data Steward.</u>"
- In Section K related to Data Consumer point 5 was updated as below (changes underlined):
    - "Maintain data confidentiality <u>as per data classification (Data classifications are defined in PS-124-ST-1)</u>."

PS-120-ST-2

- In section C SOD Controls, the following bullet point was removed:
    - "Employees cannot authorize processes that result in their own personal gain."

PS-120-ST-3

- Point E was clarified to provide examples for specific trainings related to compliance.
- PS-08 was added as a reference related to disciplinary actions in Point G.

PS-120-ST-4

- Point E was updated to reflect IT Governance resolution as below:
    - "All policies and standards must follow University processes of policy review and approval. However, all new and/or updated policies and standards must also be

reviewed by IT Governance Council (ITGC) subcommittees – Department IT Subcommittee and Research Technology Subcommittee, and Ad-hoc Faculty Senate IT Committee (FS IT Committee) prior to being submitted to ITGC for review and approval. Where applicable, stakeholders such as Subject Matter Experts, functional/technical teams impacted by policies, etc., should be included in the review process for new and/or updates to policies and standards. Any changes to baselines must be reviewed by LSUAM ITGC and/or its designee."

- A sub-point was added to Point F in relation to exception:
    - "If an exception request is denied, the submitter of the request can appeal the decision to the panel of Chairs and/or designee of Department IT Subcommittee, Research Technology Subcommittee, and Ad-hoc Faculty Senate IT Committee (FS IT Committee)"

PS-121

Policy Statement

- The word parameter was replaced with standards in all three policy statements.

PS-121-ST-1

- Added a definition of Usage activity –
    - "Logs that identifies a user and/or system (for example, user login to a network, system, or application, network device registration, etc.), as well as any actions performed by the user and/or system (for example, network access to another system or website, installation, or uninstallation of an application, etc.), while utilizing a network, system, and/or application."
- Section A, point 1 was rephrased as (changes underlined) "University network resources shall not be utilized to transmit any digital media that violates any University policies, local, state, or federal law."
- Section A, point 4 was as below (changes underlined).
    - "LSUAM must implement appropriate processes and procedures, as well as ensure technical infrastructure is implemented to provide network usage activity to support investigations conducted by authorized parties and/or to respond to legal requests as outlined in Usage Activity and Hosted Content Review section in PS-121-ST-2."
- Section E, point 1 – "is strictly prohibited" is replaced by "is prohibited, unless approved by ITSP."

PS-121-ST-2

- Section A, point 1 was rephrased to state the following:
    - "Users must properly log off and/or password protect any University owned IT assets when leaving the immediate work area for any extended length of time, for example, time-based logoff, password protected screen saver, etc."
- Section A, point 3, the following was removed:
    - "i.e., minimum level of access shall be granted to users which is required by them to perform their job duties."
- Section B, point 1 was removed:

    - "Data created on LSUAM information systems shall be deemed the property of the University unless otherwise stipulated by intellectual property agreements or other legal arrangements with the University."
- Section D, point 1.c., was rephrased as below:
    - "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."
- Section E heading was changed to "Usage activity and Hosted Content Review"
    - Point 1 was rephrased as below:
        - "All usage activities related to the use of the University networks, systems, and applications, as well as hosted content on university owned systems and/or provided applications (for example, University e-mail, Moodle, University provided storage solutions, Workday, etc.) are subject to examination by the University where:
            - An investigation has been initiated related to a formal accusation of misconduct under the University policies, or reasonable suspicion of violation of state and federal laws.
            - It is necessary to comply with or verify compliance with state or federal law, including eDiscovery procedures.
            - It is necessary to identify and/or validate security incident.*
            - It is necessary to troubleshoot technical issues.*"
    - The following sub-point was removed for Point 2 and added as a new point under the section:
        - "List of individuals or entities that can request a review of usage activity"
    - New point 3 as added as below:
        - "Usage activity review and/or hosted content review can be requested in writing by the following groups:
            - Office of General Counsel
            - Office of Human Resources
            - Office of Internal Audit
            - Office of Student Advocacy and Accountability
            - LSU Police Department"
    - A clarification/footnote was added in relation to Point 1 – "ITS can access usage activity for troubleshooting and/or security incident response. These requests are governed by standard operating procedures."

PS-121-ST-3

- The definition of DCS was modified to state – "Digital Communication Services (DCS) – DCS is any digital service/application that allows two or more people to communicate via text, audio, video, or any combination of these, but does not include communication services provided by a cellular, landline, or Voice-over-IP (VoIP) service provider or by the associated telephone device vendor. Examples include, but are not limited to, email, instant messaging, IRC, video conferencing software or websites, etc."

- Definition of Software as a Service (SaaS) was added as – "The capability provided to a consumer to access or use a provider's application running in a cloud infrastructure. SaaS can also be referred to as Cloud Application."
- Section A, point 2 was rephrased as below:
    - "All University applications (for example, Box, Adobe Creative Cloud, Workday, etc.) must be configured to utilize University provided Single Sign On services where applicable."
- Section B title was changed from Software installation, usage, and removal to Software acquisition.
- Section B point 1 was added for Software installation and usage. A list of pre-approved exceptions for Software Acquisition for local software was added as below:
    - "Software bundled with operating system acquisition that are governed by licensing terms of the operating system itself.
    - Software components, included with purchased hardware (or to be downloaded from the hardware manufacturer or designated distributor), designed specifically for the purpose of enabling the functionality of that purchased hardware when utilized in accordance with the associated license. At the time of acquisition, operating system, and software components, must be the supported by their manufacturer(s).
    - Legally obtained software for evaluation purposes in an individual, non-instructional setting for at most 30 days, provided the individual complies with all terms and conditions of the vendor's license.
    - Legally obtained freeware (i.e., no cost non-open-source software) acquired for non-administrative academic purposes in an individual, non-instructional setting in accordance with all license terms and conditions provided the license moreover:
        - allows for the software to be utilized by an enterprise entity such as LSUAM and is not exclusively a personal use license.
        - allows for the data being utilized within the software to remain under the ownership of the University and/or appropriate Data Functional Owner and is not subject to any ownership rights by the manufacturer/provider of the freeware software.
    - Legally obtained open-source software for an individual, non-instructional setting, provided it is used solely in accordance with all terms of any accompanying license, including terms and conditions including but not limited to, modification, distribution, etc.
        - Note: When students are instructed to use open-source software for course work, such software must comply with PS-31 (Digital Resources and Content Accessibility) and follow Software Acquisition process.
    - Legally obtained codes developed and/or utilized for research or instructional purposes used solely in accordance with all terms of any accompanying license or instructions.
        - Note: Any codes provided to students in an instructional setting should be in compliance with PS-31.

    - Legally obtained libraries (e.g., R package, Python module, C library, etc.) used in programming activities, used solely in accordance with all terms of any accompanying license.
    - Any software that has been approved as part of Software Acquisition Process and is on the current list of approved software published by ITS for the intended use case (e.g., instructional, administrative, research, etc.)."
- Section B point 2 was added for Software as a Service (SaaS) acquisition. The content of the subsection is as below:
    - For the purposes of this policy SaaS does not include social media sites (e.g., LinkedIn, Facebook, etc.); however, any business subscriptions for such sites are in scope (e.g., LinkedIn Recruiter).
    - As per PM-50, software subscriptions/licenses for any cloud applications, regardless of cost, utilized to conduct university business that involve private and/or confidential data or purchased using University funds must not be utilized and/or acquired without appropriate review and approval as outlined in the University processes for Software Acquisition. Cloud applications must be utilized in accordance with all license terms and conditions provided the license moreover:
        - Allows for the cloud applications to be utilized by an enterprise entity such as LSUAM and is not exclusively a personal use license.
        - Allows for the data being utilized within the cloud application to remain under the ownership of the University and/or appropriate Data Functional Owner and is not subject to any ownership rights by the cloud application provider.
- Section B point 3 was rephrased as below:
    - "Users must not disable or uninstall endpoint protection software on any University owned IT asset. Users and/or appropriate support personnel can coordinate with LSU IT Security and Policy Team (ITSP) to temporarily disable endpoint protection software for troubleshooting purposes or to add exceptions for specific applications."
- Section D point 1 was rephrased as below:
    - "Users must not knowingly install Malware on University owned IT assets. Academic research and teaching activities focused on the very topics of malware analysis, reverse engineering, etc., must restrict such activities to an environment that is completely isolated (physically or virtually) both from the LSUAM network and from the broader internet. Please refer PS-121-ST-1 for additional information."
- Section E had major modifications and the following are the new points in the section:
    - Use of DCS for University business is subject to all University policies.
    - When using DCS to conduct University business, and when the communication is initiated by an LSU user, University provided and/or approved DCS should be utilized. When using DCS to conduct University business involving private and/or confidential data, and when the communication is initiated by an LSU user, University provided and/or approved DCS must be utilized.

- As per L.R.S 44:1, communications through DCS related to university business can be subject to public records or legal requests and it is the responsibility of the University and/or individual users to respond to such requests appropriately.
- Section E point 4 required additional clarification language as below:
  - "Academic activities, including research, that engage with such content are allowed provided such activities do not violate any University policies, local, state, or federal law."

PS-124

Policy Statement

- Section A, point 1 was rephrased as below:
  - "LSUAM must establish and maintain a Data Governance Framework through a subcommittee under the purview of LSUAM IT Governance. The responsibilities of the subcommittee must be defined by IT Governance.
- Section B, point 3 was added as below:
  - "LSUAM shall define processes and procedures for disposal of data, as per data classification."

PS-124-ST-1

- Removed original Point A that referenced Data Governance subcommittee as it was moved to policy statement.
- Changed Public Data to Discretionary Data.
- Compressed the Appendix A table to clearly outline the description of different data classification as below:

	Confidential Data (highest, most sensitive)	**Private Data (moderate level of sensitivity)**	**Discretionary Data (low level of sensitivity or public)**
Description	Data and/or set of data elements that requires the highest level of security and governance. Governance of such data is typically driven by regulations (e.g., FERPA, GLBA, HIPAA, etc.) or when unauthorized disclosure, destruction, or	Data and/or set of data elements that requires moderate level of security and governance as defined by contractual obligations, University policies, etc., or when unauthorized disclosure, destruction, or modification of such data poses a	Data and/or set of data elements that is already published to the public or internally held data that may be published to the public at the discretion of the Data Functional Owner. Unauthorized disclosure, destruction, or modification of

	modification of such data poses a significant risk to the University.	moderate risk to the University.	such data poses a low risk or poses little harm to the University.

- Removed 89 numbers as an example of Confidential Data
- Added the following as an example for Discretionary Data – "Not publicly available research and/or instructional notes and manuscripts."

PS-124-ST-2

- Section B – removed the following statement:
  - "LSUAM must establish processes and procedures to disclose public data and the means through which disclosure can happen."
- Section C, point 5 – the following was removed:
  - "Any authorized access will result in disciplinary action, up to and including termination."
- Section C, point 6 was rephrased as below:
  - "Users with authorized access to private and/or confidential data should not maintain copes of such data outside of the scope of their responsibilities."
- Section D, point 1 was rephrased as below:
  - "Private and/or confidential data must only be stored on approved systems and applications (Please refer Appendix A). Electronic copies, including backups, should be kept to a minimum. Please refer to PS-133-ST-5 for Backup Management."
- Section D, point 3 was rephrased as below:
  - "When private and/or confidential data is shared, the recipient must be informed of its data classification and the need to maintain confidentiality and integrity of such data. The recipient may still disclose the information if such disclosure must be done in accordance with other University policies, local, state, and/or federal law."
- Appendix A was updated to provide clarification on the University provided Box solution. The following was also added as an Approved Storage Locations:
  - "University owned encrypted end user computing devices or encrypted on-premises storage solutions supported by ITS and/or departments."

PS-124-ST-3

- Section A, point 2 was rephrased as below and split into two points:
  - "Private and/or confidential data, should only be stored on approved systems and applications (please refer to Appendix A in PS-124-ST-2). Storage of private and/or confidential data on a user's personal asset should be avoided. If it cannot be avoided, then please refer to PS-132-ST-5 MDM and BYOD which refers to Bring Your Own Device security requirements."
  - "Electronic copies, including backups, of private and/or confidential data should be kept to a minimum. Please refer to PS-133-ST-5 for Backup Management."
- Section A, point 7 was removed and combined with point 2.
- Section B point 1 was rephrased as below:

- "LSUAM must define appropriate assessments to be conducted which will help in development of…"

PS-124-ST-4

- Added definition of personal information:
  - "An individual's first and last name with any one or more of other identifiable data elements including, but not limited to, Driver License, Social Security Number, Date of Birth, Credit and/or Debit Card number (with any required security code, access code, or password), Bank account information, Passport Number, and Biometric data."
- Point 6, 7, and 8 were combined and rephrased as below:
  - "LSUAM must establish University level processes and procedures to:
    a. Provide access to Users to the personal information collected from them.
    b. Allow users to review, update, and correct any personal information collected and stored.
    c. Allow users to remove collected personal information, where applicable.

    NOTE: individual departments/units/LSU employees responsible for collected data can also address such requests, where applicable."

PS-126

Policy Statement

- Points 2, 3, and 4 were restructured as below:
  - Wherever encryption is used:
    - Encryption of data should only be carried out using National Institute of Standards and Technology (NIST) approved and/or commercially supported encryption algorithms.
    - Encryption keys must be generated, stored, accessed, distributed, and destroyed in a controlled and secured manner as defined in PS-126-ST-1.
    - Encryption keys must be periodically changed as defined in PS-126-ST-1.

PS-126-ST-1

- Definition of Data encryption key and Key Exchange Keys.
- The following note was added to A.1.
  - "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."
- Section A, point 2 – "system" was replaced with "servers, storage systems" and examples were added for portable/removable media.
- Section B, point 1 – the term "over the network" was added to add clarification for transmission of data. Additionally, reference to PS-124-ST-2 was added.
- Section B, point 2 was moved lower in the section and is now the new Point 6.

- Section B, point 3 (new point) was rephrased as – “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.”
- 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.”
- The following was added to the Section C heading – “(for system and application administrators)”
- Section C, point 1 – 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.”
- Section C, point 2 – specific key lengths were removed, and the statement was rephrased as – “The following symmetric algorithms with the recommended and supported key lengths…”
- Section C, point 5 – clarification was added that the statement relates to “for sites associated with the University”.
- Section D, point 1 – the following was added at the end of the statement:
    - “and offer it to departments, units, and/or individuals for management of encryptions keys.”
- Section D, point 2 was rephrased as – “Where encryption is being managed at the unit level, each unit identify Key Managers and Key Custodians and where feasible, these duties should be segregated.”
- Section D, point 3 the following was added – “For example, storing an encryption key in secure and encrypted storage solutions, such as University provided Box and/or OneDrive solutions or enterprise key management solution, etc.
- Section D, point 5 was modified as – “University provided encryption solutions must log and document all key management activities to ensure an appropriate audit trail is maintained.”
- Section D, point 6 the following was added – “Where encryption is being managed at the unit level, units must develop similar processes and procedures.”
- Section D, point 10 was rephrased as – “When encrypted data is transmitted, any password, passphrases, and keys associated with encrypted data must be sent separately using secure methods only (TLS, IPSec, SFTP, encrypted email, etc.). For example, using files-to-geaux solution to share encrypted information, the link can be shared via one channel (Teams Message), while the password should be shared via encrypted email.”
- Section D, point 11 was rephrased as – “Where asymmetric encryption is utilized for data in transit, the public and private key pair should be changed every three years or sooner if there is a reasonable suspicion that the keys have been compromised.”
- Section D, point 12 was reordered as below:
    - “Where symmetric encryption is utilized:
        - Data Encryption Keys for data at rest shall be changed at least every three years. The key should be changed sooner if there is a reasonable suspicion that the key has been compromised. This does not include full-disk encryption technologies being utilized.

        - System/application developers should ensure that Data Encryption Keys for data in transit be changed, at a minimum, once per session or every 24 hours whichever is shorter.
        - Master keys are to be changed, at a minimum, annually. This would generally be applicable for encryption key management solutions.
        - System/application developers should ensure that Key Exchange Keys be changed, at a minimum, twice a year."
- Section D, point 14 was rephrased as – "Changes to role of key custodians, such as separation from the University and/or move to positions outside a unit, shall result in key revocation and replacement of encryption keys managed by the key custodian."

All policies and standards

- The following section and language have been added to almost all policy statements:
    - EXCEPTIONS AND NON-COMPLIANCE
        - Please refer PS-120-ST-4 for additional information related to exceptions.
        - Please refer PS-120 for additional information related to Policies and Standards non-compliance.
- The word parameter has been replaced with standard.
- The word sensitive information has been replaced with private and/or confidential data.