SAN JOSÉ STATE UNIVERSITY
ONE WASHINGTON SQUARE
SAN JOSE, CA 95192

SS-F18-3, Sense of the Senate Resolution, Advocating Additional Protections for the Privacy of Electronic Information at San José State University

Legislative History: At its meeting of October 1, 2018, the Academic Senate approved the following Sense of the Senate Resolution presented by Senator Peter for the Professional Standards Committee.

SENSE OF THE SENATE RESOLUTION
Advocating Additional Protections for the Privacy of Electronic Information at San José State University

Resolved: That the Academic Senate thanks the President for her detailed veto message of S17-8 which made possible a compromise recommendation (conveyed separately); be it further

Resolved: That through this resolution the Academic Senate records its continued support for those privacy protections contained in S17-8 that were deleted to conform with the President's message. We hold that those provisions are consistent with commonly accepted standards for the protection of privacy at universities. We are concerned that SJSU faculty, staff, and students will have a lower level of privacy protection than their counterparts at the University of California (UC)[i] and a lower level of protection than that recommended by the American Association of University Professors (AAUP.)[ii] Be it further

Resolved: That the Academic Senate finds that system wide "Responsible Use Policy"[iii] lacks the safeguards needed to adequately protect privacy to the reasonable levels recommended by the AAUP or enacted by the UC.[iv] Consequently, we find that augmentation by a supplemental campus policy (as provided for in the CSU Responsible Use Policy) is required;[v] be it further

Resolved: That our concerns could be allayed by the incorporation of certain commonly accepted privacy protections into the Presidential Directive

referred to in the (new) policy setting forth “Principles Regarding Privacy of Electronic Information.”

1. SJSU should adopt rules that make the invasion of privacy of faculty, staff, and students a rare event and one that only takes place under circumstances that are carefully defined and published. Every member of the SJSU community should know the circumstances under which their communications and records may be searched or disclosed without their consent or without their knowledge.[vi]

2. SJSU should adopt rules that identify who shall be responsible for authorizing any involuntary search, and should keep clear records of each search that is authorized and the rationale for doing so.[vii]
3. SJSU should adopt rules that limit the involuntary searching or disclosure of information to the least perusal of contents and the least action necessary to resolve a given matter.[viii]
4. SJSU should adopt rules that require disclosure of involuntary searches to the individuals involved, following the conclusion of the investigation and subject to any legal requirements.[ix]
5. SJSU should adopt rules that promote accountability for acts of involuntary disclosure. This should include some mechanism for internal oversight by a responsible party who is not responsible for authorizing the searches.[x]
6. SJSU should adopt rules that promote transparency and accountability in the design and implementation of any analytic systems that gather, use, and/or store data about SJSU community members. For example, consider adopting the suggestions provided by the Association for Computing Machinery US Public Policy Council (USACM).[xi]

Rationale:

On April 20, 2018, President Papazian returned (vetoed) S17-8, which was a policy recommendation designed to secure privacy protections for electronic information at SJSU commensurate with those in place currently in the University of California system, and similar to those recommended in its white paper by the American Association of University Professors (AAUP.) Current policies pertinent to privacy of electronic information at SJSU include our obsolete campus policy (F97-7) and the CSU system “Responsible Use Policy.”

In order to foster a cooperative relationship with the President and our campus Administration, the Academic Senate has produced a new policy recommendation that conforms to the instructions in the veto message. However, we continue to believe that stronger privacy protections—similar to those initially proposed--are warranted, and propose this resolution to record our support for those protections. We hope that these protections can be included in the expected Presidential Directive.

Attached to this resolution are the documents needed to understand the development of this issue:

1. *F97-7 Privacy of Electronic Information and Communications*
2. *S17-8 Privacy of Electronic Information (unsigned)*
3. *Memo From Mary Papazian RE: "Policy Rescinding and Replacing F97-7 on Privacy of Electronic Information (S17-8)*
4. *Electronic Communications Policy. University of California, Office of the President.*
5. *"Academic Freedom and Electronic Communications," AAUP*
6. *CSU Responsible Use Policy.*

Approved: *September 10, 2018*

Vote: *9-0-2*

Present: *Chin, Kumar, He, Monday, McKee, Cargill, Peter, Hart, Kemnitz, Rodriquez, Mahendra*

Absent: *None*

Financial Impact: *No direct impacts*

Workload Impact: No direct impacts

Endnotes:

[i] Electronic Communications Policy; University of California Office of the President. Issued November 17, 2000. Revised August 18, 2005.

[ii] "Academic Freedom and Electronic Communications." See especially section IX. American Association of University Professors Committee A on Academic Freedom and Tenure, revised November 2013. "Faculty members should be involved in the setting of

institutional policies surrounding the monitoring of and access to content and traffic data in electronic communications" (page 55.)

[iii] California State University. "Responsible Use Policy." Last revised 6/5/2013.

[iv] The Responsible Use Policy does reference privacy in its provisions 3.6, 3.9, and 4.3. While welcome, these protections are vague and fail to meet the standards of the UC or AAUP. For example, "The CSU supports and protects the ***concepts*** of privacy…" or "the CSU does not ***generally*** monitor or restrict content…" (emphasis added.)

[v] The Responsible Use Policy specifically allows for campus supplemental policies. "2.2 The policy may be augmented, but neither supplanted nor diminished, by additional policies and standards adopted by each campus."

[vi] AAUP states "The policy should clearly state that the university does not examine or disclose the contents of electronic communications and traffic data without the consent of the individual participating in the communication except in rare and clearly defined cases" (page 54.)

UC system policy states "An electronic communication holder's consent shall be obtained by the University prior to any access for the purpose of examination or disclosure of the contents of University electronic communications records in the holder's possession, except as provided for below" and then lists four specific exceptions (pages 10-11.)

CSU San Marcos's *Acceptable Use of Information Technology Resources* policy (9/7/2016) contains an "Information Privacy" section contains similar language "The consent of an electronic communication holder or account owner shall be obtained prior to the inspection, capture or disclosure of the contents of electronic communication records except as provided…" followed by a list of legal exceptions.

[vii] AAUP states "Policies on electronic communications should enumerate narrow circumstances where institutions can gain access to traffic logs and content unrelated to the technical operation of these services. If a need arises to get access to electronic-communications data, a designated university official should document and handle the request, and all parties to the communication should be notified in ample time for them to pursue protective measures—save in the rare case where any such delay would create imminent risk to human safety or university property" (page 55.)

UC system policy states "such actions must be authorized in advance and in writing by the responsible campus Vice Chancellor…" (page 11.)

[viii] AAUP states "Accessed data may not be used or disseminated more widely than the basis for such exceptional action may warrant" (page 55.)

UC system policy states "In emergency circumstances as defined in Appendix A, Definitions, the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately…."

[ix] UC system policy states “The responsible authority or designee shall at the earliest opportunity that is lawful and consistent with other University policy notify the affected individual of the action(s) taken and the reasons for the action(s) taken.

[x] UC system policy states “Each campus will issue in a manner consistent with law an annual report summarizing instances of authorized or emergency nonconsensual access pursuant to the provisions of this Section IV.B Access Without Consent, without revealing personally identifiable data.”

[xi]The Statement on Algorithmic Transparency and Accountability, Association for Computing Machinery US Public Policy Council (USACM), January 12, 2017.