UCSF Academic Senate

http://senate.ucsf.edu

Office of the Academic Senate
500 Parnassus Ave, MUE 230
San Francisco, CA 94143-0764
Campus Box 0764
tel: 415/514-2696
academic.senate@ucsf.edu
https://senate.ucsf.edu

Ruth Greenblatt, MD, Chair
David Teitel, MD, Vice Chair
Arthur Miller, PhD, Secretary
Jae Woo Lee, MD, Parliamentarian

July 18, 2017

Jim Chalfant, PhD
Chair, Academic Council
Systemwide Academic Senate
University of California Office of the President
1111 Franklin St., 12th Floor
Oakland, CA 94607-5200

Re: Review of Revised Presidential Policy on Electronic Information Security (IS-3)

Dear Jim,

The San Francisco Division of the Academic Senate has reviewed the proposed revisions to the Presidential Policy on Electronic Information Security (IS-3). After review and discussion, the Senate's Executive Council, along with the Committee on Academic Planning and Budget (APB) and the Committee on Academic Freedom (CAF), has concerns over existing Section 1.2.2, *Costs of an Information Security Incident.* According the current policy, "Units will bear the direct costs that result from an Information Security Incident under the Unit's area of responsibility that resulted from a significant failure to comply with this policy. The costs include, but are not limited to: the response, containment, remediation, forensics, analysis, notification, litigation, penalties, regulatory fines and any other costs directly attributable to the Information Security Incident."

Given the ever-changing IT security risks and the attendant high costs associated with security breaches, it is unreasonable to hold individual faculty financially liable for breaches that occur while performing the work of the university. At a minimum, there should be more specificity on the definition of what would constitute a "unit" involved in such a breach. For instance, what is the smallest entity that would constitute a unit? With respect to individual liability, the UCSF Senate is also concerned that there may not be any limits to personal financial liability for faculty under this policy. Indeed, it is our understanding that such costs would be typically covered under an institutional Information Technology insurance policy, that UC presumably already holds.

With respect to improving the existing Section 1.2.2, UCSF's CAF has submitted the following suggested revisions (additions in **bold underline**):

"Units ~~**will**~~ **may** bear the direct costs that result from an Information Security Incident under the Unit's area of responsibility that resulted from a significant failure to comply with this policy. **A "significant failure to comply with this policy" includes repeated failures to apply information security policies, procedures, standards and best practices, and/or attempt to gain unauthorized access, disrupt operations, gain access to confidential information security strategies or inappropriately alter Institutional Information.** The costs include, but are not limited to: the response, containment, remediation, forensics, analysis, notification, litigation, penalties, regulatory fines and any other costs directly attributable to the Information Security Incident."

Thank you for the opportunity to review the proposed changes to this important Presidential policy. If you have any questions on UCSF's comments, please do not hesitate to let me know.

Sincerely,

Ruth Greenblatt, MD, 2015-17 Chair
UCSF Academic Senate

Encl. (2)
CC: David Teitel, Vice Chair, UCSF Academic Senate
Chad Christine, UCSF APB Chair
Brent Lin, UCSF CAF Chair

UCSF Academic Senate

http://senate.ucsf.edu

Communication from the Academic Planning and Budget Committee

Chad Christine, MD, Chair

June 20th, 2017

TO: Ruth Greenblatt, Chair of the UCSF Division of the Academic Senate

FROM: Chad Christine, Chair of the Academic Planning and Budget Committee

RE: Review of the Proposed Revisions to the Presidential Policy on Electronic Information Security

Dear Chair Greenblatt:

The members of the Academic Planning and Budget (APB) Committee have reviewed proposed revisions to the Presidential Policy on Electronic Information Security. After review and discussion, members have determined that we do not have any comments on the proposed changes. However, there are concerns with existing Section 1.2.2 Costs of an Information Security Incident. According the current policy, “Units will bear the direct costs that result from an Information Security Incident under the Unit’s area of responsibility that resulted from a significant failure to comply with this policy. The costs include, but are not limited to: the response, containment, remediation, forensics, analysis, notification, litigation, penalties, regulatory fines and any other costs directly attributable to the Information Security Incident.” According to the policy, “Units” are described as, “A generic term for Dean, Vice Chancellor or similar senior role who has the authority to allocate budget and is responsible for Unit performance. At a particular location or in a specific situation the following senior roles may also be Unit Heads: department chairs, assistant/associate vice chancellor (AVC), principal investigators, directors or senior managers.”

APB members believe that with ever-changing IT security risks and the attendant high costs associated with security breeches, it is unreasonable to hold individual faculty financially liable for breaches that occur while performing the work of the university. APB encourages the Academic Senate advocate for a policy revision that indemnifies individual faculty from the costs associated with IT security incidents.

We propose the Executive Council invite UCSF’s CIO Joe Bengfort to clarify the proposed IT Policy. The following questions should be addressed:

- Who defines the Unit responsible for cyber security breach?
- What is the smallest Unit that could be held responsible?
- Are there limits to the magnitude of financial responsibility (e.g. $5K, $100K)?

Sincerely,

Chad Christine, MD
Chair of the Academic Planning and Budget Committee

UCSF Academic Senate

http://senate.ucsf.edu

Communication from the Committee on Academic Freedom
Brent Lin, DMD, Chair

26 June 2017

Ruth Greenblatt, MD, Chair
UCSF Academic Senate
500 Parnassus Avenue,
San Francisco, CA

Re: CAF Comments on the Review of Revised Presidential Policy on Electronic Information Security (IS-3)

Dear Chair Greenblatt,

At its most recent meeting, the Committee on Academic Freedom (CAF) reviewed the *Revised Presidential Policy on Electronic Information Security (IS-3)*, and discussed the changes to the policy with Pat Phelan, Information Security Director at UCSF. While much of the policy seems appropriate, CAF is concerned with section 1.2.2, Costs of an Information Security Incident, which states that "units will bear the direct costs that result from an Information Security Incident under the Unit's area of responsibility that resulted from a significant failure to comply with this policy." CAF's particular concern is that an affected unit may pass down these costs to a faculty member who may have been responsible for the security breach. Although this section seems to apply to blatant transgressors of this policy (e.g., those who have deliberately chosen not to encrypt laptop computers, failure to install BigFix, etc.), CAF is suggesting the following changes in the language within this section (additions in **bold underline**) to :

> Units ~~**will**~~ **may** bear the direct costs that result from an Information Security Incident under the Unit's area of responsibility that resulted from a significant failure to comply with this policy. **A "significant failure to comply with this policy" includes repeated failures to apply information security policies, procedures, standards and best practices, and/or attempt to gain unauthorized access, disrupt operations, gain access to confidential information security strategies or inappropriately alter Institutional Information.** The costs include, but are not limited to: the response, containment, remediation, forensics, analysis, notification, litigation, penalties, regulatory fines and any other costs directly attributable to the Information Security Incident.

If you have any questions on CAP's comments, please do not hesitate to let me know.

Sincerely,

Brent Lin, DMD
CAF Chair