



Jim Chalfant
Telephone: (510) 987-0711
Fax: (510) 763-0309
Email: jim.chalfant@ucop.edu

Chair of the Assembly of the Academic Senate
Faculty Representative to the Regents
University of California
1111 Franklin Street, 12th Floor
Oakland, California 94607-5200

August 3, 2017

SUSAN CARLSON, VICE PROVOST
ACADEMIC PERSONNEL

Re: Revised Presidential Policy on Electronic Information Security

Dear Susan:

As you requested, I distributed for systemwide Senate review the revised Presidential Policy on Electronic Information Security (IS-3). Six Academic Senate divisions (UCD, UCI, UCM, UCR, UCSB, UCSC, and UCSF) and three systemwide committees (UCFW, UCPB, and UCORP) submitted comments. These comments were discussed at Academic Council's July 26, 2017 meeting. They are summarized below and attached for your reference.

The Academic Senate cannot support the current version of the policy due to a number of significant concerns about its clarity, length, accessibility to a general readership of faculty end-users, and its potential compliance implications for faculty. Senate reviewers agree that the policy requires a thorough revision.

We understand that the goals of the revisions are to bring UC into compliance with new federal requirements related to faculty research contracts and to replace inconsistent campus policies with a single systemwide framework for responding to the risk of security breaches. This framework includes a minimum security baseline that aligns with international standards, but also provides UC campuses with flexible options for meeting the standards and includes principles to guide the development of local security programs and campuses' allocation of resources to target risk priorities.

Senate reviewers' dominant concern is that the policy is overly technical and vague. Many reviewers noted that it fails to use plain English and to adequately define key technical terms in a way that faculty without a specialized background can easily understand its basic provisions and implications.

The policy is also ambiguous concerning the respective roles and responsibilities of different campus authorities in implementing and overseeing the policy, particularly the specific tasks for which faculty will be responsible under the policy, as well as the expected relationship between

campus authorities and between campus authorities and UCOP. Several reviewers interpreted the overall position of the policy in this regard as delegating authority to the campuses to set individual information security policies, noting that the policy is helpful only to the extent that it does allow campuses to develop and implement their own policies. However, these goals are unclear, and resolving this vagueness should be one of the first priorities for clarification.

Several Senate reviewers observed that the policy would apply to “all devices, independent of their location or ownership, when connected to a UC network or cloud service used to store or process Institutional Information.” In other words, the policy does not distinguish between computers, cell phones, and other electronic devices that are UC-owned, and devices that are personally-owned. Reviewers noted that full compliance with these provisions would be impractical, and more importantly, could threaten faculty privacy and autonomy. They also noted that data from large grants and identifiable human subjects would be classified at the highest security levels (P3 and P4), which suggests that many faculty, teaching assistants, graduate students, and undergraduates would be subject to background checks. Reviewers felt that it would be more practical to focus the policy on UC-owned systems.

Reviewers noted several other specific aspects of the policy that require additional clarification or development. These include the need to clarify the role of the IRB in performing risk assessments, classifying information, and evaluating appropriate electronic information protections; the need for the policy to account for the common practice of sharing customized code between UC faculty and researchers at other institutions; and the potential for costs from an information security incident in a unit to be passed onto individual faculty members.

We appreciate consideration of our comments and concerns as you revise the proposed policy. Please do not hesitate to contact me if you have further questions.

Sincerely,



Jim Chalfant, Chair
Academic Council

Encl

Cc: Academic Council
CIO Andriola
Director Smith
Senate Director Baxter
Senate Executive Directors



DAVIS DIVISION OF THE ACADEMIC SENATE
ONE SHIELDS AVENUE
DAVIS, CALIFORNIA 95616-8502
(530) 752-2220
academicsenate.ucdavis.edu

July 17, 2017

Jim Chalfant

Chair, Academic Council

RE: Draft Revised Presidential Policy on Electronic Information Security (IS-3)

Dear Jim:

The Davis Division received the draft revised Presidential Policy on Electronic Information Security (IS-3) and sent it to the Committee on Information Technology (CIT) for initial review. Based on CIT feedback, the Davis Division believes the draft is not ready at this time to forward to our committees for broader review. As currently written, the draft is too dense and is inaccessible to a wide, non-information technology audience.

The Davis Division will await a more readable draft of the policy before distributing widely for review.

Sincerely,

A handwritten signature in cursive script that reads "Rachael E. Goodhue".

Rachael E. Goodhue

Chair, Davis Division of the Academic Senate

Professor and Chair, Agricultural and Resource Economics

c: Edwin M. Arevalo, Executive Director, Davis Division of the Academic Senate
Hilary Baxter, Executive Director, Systemwide Academic Senate
Michael LaBriola, Principal Policy Analyst, Systemwide Academic Senate



Office of the Academic Senate
307 Aldrich Hall
Irvine, CA 92697-1325
(949) 824-2215 FAX

June 22, 2017

Jim Chalfant, Academic Council
1111 Franklin Street, 12th Floor
Oakland, CA 94607-5200

RE: Systemwide Senate Review of Revised Presidential Policy on Electronic Information Security (IS-3)

Dear Jim,

At its meeting of June 20, 2017, the Irvine Division Senate Cabinet reviewed the proposed revisions to the Presidential Policy on Electronic Information Security (IS-3). The Council on Research, Computing, and Libraries and the Council on Faculty Welfare initially reviewed the proposed revisions. The Irvine Division Senate Cabinet has no specific concerns with the proposed revisions.

The Irvine Division appreciates the opportunity to comment.

Sincerely,

A handwritten signature in cursive script that reads "Bill Parker".

Bill Parker
Irvine Division Senate Chair

C: Maria Pantelia, Chair-Elect, Academic Senate, Irvine Division
Hilary Baxter, Executive Director, Academic Senate
Natalie Schonfeld, Executive Director, Academic Senate, Irvine Division

UNIVERSITY OF CALIFORNIA, MERCED

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO



SANTA BARBARA • SANTA CRUZ

OFFICE OF THE ACADEMIC SENATE
SUSAN AMUSSEN, CHAIR
senatechair@ucmerced.edu

UNIVERSITY OF CALIFORNIA, MERCED
5200 NORTH LAKE ROAD
MERCED, CA 95343
(209) 228-7954; fax (209) 228-7955

JULY 14, 2017

JIM CHALFANT, CHAIR, ACADEMIC COUNCIL

RE: DRAFT REVISED PRESIDENTIAL POLICY ON ELECTRONIC INFORMATION SECURITY (IS-3)

The Merced Division's Committee on Research was asked to review the draft revised *Presidential Policy on Electronic Information Security (IS-3)*, as the policy arrived after the Divisional Council's last meeting. The committee's thoughtful and comprehensive comments are appended for Academic Council's consideration, and represent the Merced Division's response to the policy.

We thank you for the opportunity to opine.

Sincerely,

A handwritten signature in cursive script, appearing to read "Susan Amussen".

Susan Amussen, Chair
Division Council

CC: Divisional Council
Hilary Baxter, Executive Director, Systemwide Academic Senate
Laura Martin, Executive Director, Merced Division

Enc (2)

UNIVERSITY OF CALIFORNIA, MERCED

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO



SANTA BARBARA • SANTA CRUZ

ACADEMIC SENATE, MERCED DIVISION
COMMITTEE ON RESEARCH
DAVID C. NOELLE, CHAIR
dnoelle@ucmerced.edu

UNIVERSITY OF CALIFORNIA, MERCED
5200 NORTH LAKE ROAD
MERCED, CA 95343
(209) 228-4369

June 30, 2017

To: Susan Amussen, Chair, Division Council

From: David C. Noelle, Chair, Committee on Research (COR) *David C. Noelle*

Re: Draft Revised Presidential Policy on Electronic Information Security

The Committee on Research (COR) was asked to comment on the revised draft of the Presidential Electronic Security Policy. The Committee appreciates this opportunity to opine on an important systemwide matter.

It is clear that an extensive amount of effort has gone into the production of this draft policy document. Supporting materials, such as the FAQ and Glossary, make for useful components of the policy. With special consideration for the research mission of the UC, there are features of this draft that start to appropriately address the complexities of maintaining electronic security and privacy in the diverse and, by principle, open situations in which research is conducted. For example, the flexibility of oversight options for researchers, including allowing a PI to directly shoulder responsibility for policy compliance, is a very welcome aspect of this policy. Still, the document remains quite vague, making it difficult to imagine how compliance might be appropriately determined. The Committee recognizes that, at least to some degree, the vague nature of this policy is intended to allow location-specific policies to be crafted with minimal arbitrary constraints. However, there is a substantial risk that the abstract nature of the document will introduce difficult ambiguities when evaluating location-specific policies. Also, the goal of allowing diversity in location-specific policies introduces obstacles for research activities spanning multiple UC campuses.

Much of this policy outlines formal positions of authority, along with corresponding responsibilities. What is frequently missing, however, is the relationships between these positions. Many key decisions are placed in the hands of single individuals, introducing a risk of bias, but there is no guidance concerning how (or if) decisions can be appealed. May the Cyber-risk Responsible Executive (CRE) overrule decisions by the Chief Information Security Officer (CISO)? Does the systemwide officer hold any further adjudication authority over the location-specific positions? Is there an appeal process for denied requests for exceptions to policy? Who determines if a Unit has failed to comply with this vague policy when assessing incident recovery costs (e.g., "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.")? Of particular importance to faculty researchers, the policy is not clear about when such researchers are to be considered to bear the authority and responsibility of Unit Heads, rather than members of the workforce. (Examples in the document suggest irrelevant criteria, such as project

funding magnitude.)

One established institution concerned with security and privacy is surprisingly missing from this policy - the Institutional Review Board (IRB) or its equivalent. In the context of the collection and maintenance of sensitive human research data, the IRB is already charged with performing risk assessments and evaluating the electronic information protections most appropriate for the experimental methods being used and the standards of the discipline. This body is well situated to take important details into account. What role does the IRB play in determining the classification of Institutional Information and evaluating appropriate security and privacy protections?

More generally, the policy does not communicate an appreciation for the full range of complications that arise from the highly networked nature of the modern world. Technologies outside of the direct control of the UC play an increasingly critical role in research productivity. The document appears to address this problem by extending UC authority in unreasonable ways. For example, the glossary indicates that the set of governed IT resources "includes both UC-owned and personally owned devices." As another example, before a researcher connects to his laboratory computers from a remote location (e.g., from an academic conference site), Section 13.1 requires the researcher to "[o]btain approval from the Location CIO for the use of the external network service provider." Expecting campus officials to inspect every remote device and every network service before allowing connectivity to UC systems is unworkable. Instead, policy should focus on UC-owned systems, aiming at incorporating automated protections that are active when those systems interact with the broader world.

Importantly, there is also a somewhat hidden danger to academic freedom embedded in this policy document. In multiple places, the document indicates that damage to "UC reputation" should be considered when making security and privacy decisions. This introduces the possibility of inappropriate use of this policy to suppress the dissemination of research results that are, explicitly or implicitly, critical of UC activities. For example, educational research might discover that some educational practices widely used at the UC are ineffective, and this policy might be used as a justification, based on risk to "UC reputation", to make it difficult to disseminate relevant research data. Such risks to academic freedom must play an important role in making security and privacy decisions.

The Committee noted a number of other points of ambiguity. For example, the document explicitly states that, "This policy does not apply to UC students." But constraints are placed on students in Section 9.2.1. Furthermore, it is not clear when a given individual should be seen as a student versus a workforce member, according to this policy. Lastly, the delegation of duties to the CIO could use some justification, as many of these might be reasonably seen as the purview of the CISO (e.g., the appointment of committee members in Section 2.3).

The Committee recognizes that generating a policy document of this kind is important to establish UC compliance in a variety of critical contexts. It is also clear that some flexibility should exist for the customization of policy on individual campuses. Still, the vague and abstract nature of this draft raises serious concerns that the appearance of compliance will mask confusion and inconsistency in the policy's implementation. These comments are offered with the hope that they will help with the fabrication of a more transparent and practical policy.

Thank you for your consideration.

cc: Senate Office



CHAIR, ACADEMIC SENATE
RIVERSIDE DIVISION
UNIVERSITY OFFICE BUILDING, RM 225

DYLAN RODRIGUEZ
PROFESSOR OF ETHNIC STUDIES
RIVERSIDE, CA 92521-0217
TEL: (951) 827-6193
EMAIL: DYLAN.RODRIGUEZ@UCR.EDU

June 28, 2017

Jim Chalfant, Chair, Academic Council
1111 Franklin Street, 12th Floor
Oakland, CA 94607-5200

RE: (Systemwide Review) Draft Revised Presidential Policy on Electronic Information Security (IS-3)

Dear Jim,

Relevant committees from the UCR Division of the Academic Senate, along with its Executive Council, discussed the Draft Revised Presidential Policy IS-3. Some significant concerns were expressed in the review.

The Committee on Library and Information Technology (LIT) expressed strong concern that it was not afforded adequate time to more thoroughly review the draft policy. It nonetheless raised several serious issues for consideration. The length of the document is onerous, and the content of the policy is inaccessible to a general faculty readership. The committee suggests the need for a document that is composed of sections directed toward particular groups of constituents/readers. Regarding matters directly affecting faculty, a number of problems were raised: section 1.2.1 does not define "serious violations;" the implementation of financial liability for failures of compliance are not defined; and more generally, the document reads as a legal one rather than a faculty-directed one. It requires thorough revision/rewriting.

Executive Council discussed the draft policy and echoed the concern about the short timeline for review, while anticipating that an opportunity for more substantive review on a future draft will possible produce a greater range and depth of comments than was provided in this round of consultation. Council supports the Committee on LIT's evaluative comments and preliminary suggestions.

The Committee on Faculty Welfare did not add anything substantial, and the Committee on Research chose not to offer an opinion.

Sincerely yours,


A handwritten signature in black ink, appearing to read "Dylan Rodriguez".

Dylan Rodríguez
Professor of Ethnic Studies and Chair of the Riverside Division

CC: Hilary Baxter, Executive Director of the Academic Senate
Cherysa Cortez, Executive Director of UCR Academic Senate Office

June 14, 2017

To: Dylan Rodriguez, Chair
Riverside Division

From: Leonard Nunney 
Committee on Library and Information Technology

Re: [Systemwide Review] Proposed Revised Policy: Draft Revised Presidential Policy on Electronic Information Security (IS-3)

The Committee on Library and Information Technology reviewed the [Systemwide Review] Proposed Revised Policy: Draft Revised Presidential Policy on Electronic Information Security (IS-3) at their June 6, 2017 meeting. We would have liked more time to deliberate on this policy document; however, some concerns were immediately apparent.

Our most obvious concern is the length of the document. It is positively encyclopedic and yet presented in a form that makes it very difficult (if not impossible) for faculty to identify pertinent information. Faculty appear to be defined under the very non-specific terms of "Unit Head" and "Workforce Manager", both of which appear to encompass a huge range of positions (in addition to faculty) that have very different perspectives and responsibilities.

We would suggest preparing a document with sections focused on different groups rather than attempting (and largely failing) to have complete generality. For example, it would be more effective if the policy clearly distinguishes faculty from the various levels of administrator, and those faculty with sensitive data (i.e. P3 and P4 information) from those who do not (i.e. only P1 and P2 information).

A number of very important issues potentially affecting faculty are glossed over. For example, it is noted in section 1.2.1 that there may be sanctions against faculty and student for "serious violations" of the policy, but the actions that constitute "serious violation" never appear to be defined. Moreover, it is stated that a Unit will bear the cost of a "significant failure to comply" (section 1.2.2). Does this mean the faculty grants or faculty individually are financially liable for any problems that occur regarding a

laboratory or office computer? Again, this issue is never expanded beyond the simple statement of potential liability.

In summary, this Policy is written as a legal document rather than a document that faculty can refer to in order to understand best practices. As such, it should be substantially revised and rewritten.



ACADEMIC SENATE
Santa Barbara Division
1233 Girvetz Hall
Santa Barbara, CA 93106-3050

(805) 893-4511
<http://www.senate.ucsb.edu>
Henning Bohn, Chair

July 3, 2017

To: Jim Chalfant, Chair
Academic Council

From: Henning Bohn, Chair
Santa Barbara Division

A handwritten signature in black ink that reads "Henning Bohn". The signature is written in a cursive style and is positioned to the right of the "From:" field.

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

The Santa Barbara Division offered 18 Senate groups an opportunity to comment on IS-3, but most opted not to opine, possibly due to the complexity of the policy and timing of the review, coupled with the full agendas that many councils and committees are generally faced with during the final months of spring quarter.

The Council on Faculty Issues and Awards (CFIA) found the policy difficult to follow due to the highly technical language and the heavy use of acronyms and commented that this, combined with an insufficient glossary, renders the document inaccessible for most non-technical readers. CFIA also found the policy to be overly broad and thus lacking in clarity as to how it would impact campus members on a daily basis. While the Council recognizes the importance of having a strong electronic security policy in place, CFIA does not support the currently proposed version of IS-3.

The Committee on Diversity & Equity (CDE) was perplexed by the vacillation between sections that referenced very specific, technical policies and sections in which the policy was extremely vague. While the revised draft is heavy on broad terms and concepts, it falls short in actually laying out the specific tasks for which campus administrators will be responsible. CDE also noted that the policy places risks on faculty interests, particularly with regard to the responsibilities of research PIs. CDE raised the following questions: 1) who is over-seeing the policy implementation on each campus, and within specific campus units; 2) how will the policy be implemented and carried out? 3) who is representing the faculty; 4) who will ensure that faculty have the campus support they will require; 5) is there any relationship between this policy and the campus-wide switch to the Google email platform; and 6) might information security be impacted by the decision to move all faculty email to a corporate, cloud-based system?

Graduate Council (GC) echoed the concerns of other groups regarding the policy's tendency to veer from very specific to overly vague, noting that clear definitions for terms such as "institutional information" and "institutional resource" are essential to ensuring faculty compliance. Members also asked the following: 1) who will oversee risk assessment; 2) how will implementation be financially viable; and 3) how will every faculty member know exactly what encryption requirements they must use? Concern was expressed that, per the revised policy, unit heads and PIs will bear the cost of an incident. GC asserted that the delegation of financial risk to unit heads and PIs could prove catastrophic for some departments and faculty members, and that this policy should be protective of faculty, rather than punitive.

The Division's Cyber Security Working Group (CSWG) commented that many non-technical readers will find the document difficult to read and suggested that the policy and language are more severe than necessary. This group expressed concerns about how the policy would impact specific types of data and data protection such as research data related to the Department of Defense and the Department of Energy. CSWG recognizes that a strong electronic information security policy is vital for the UC and, despite its concerns, supports the Revised Presidential Policy of Electronic Information Security (IS-3).

The College of Engineering Faculty Executive Committee was somewhat confused as to the differences between the current policy and the proposed revised policy and therefore requested a one-page executive summary identifying these differences.

In summary, all non-specialist reviewing groups (all but CSWG) had serious concerns and questions. Hence, the Santa Barbara division cannot support the proposed policy.



1156 HIGH STREET
SANTA CRUZ, CALIFORNIA 95064

Office of the Academic Senate
SANTA CRUZ DIVISION
125 CLARK KERR HALL
(831) 459 - 2086

July 19, 2017

JIM CHALFANT
Chair, UC Academic Council

Re: Systemwide Review of Draft Revised Presidential Policy on Electronic Information Security

Dear Jim,

The Santa Cruz Division has reviewed and discussed the draft revised Presidential Electronic Information Security Policy. Responses were received from the Committees on Academic Freedom (CAF), Information Technology (CIT), and Library and Scholarly Communication (COLASC).

We appreciate the Office of the President's efforts to develop a policy that will provide a security framework to respond intelligently to the ever increasing risk of security breaches. The revised policy is highly technical and quite vague in places, and therefore it was difficult to evaluate whether the proposed changes were substantially different from the previous IT security guidelines. It appears that the policy will not impact academic freedom, although the expansive scope of the policy raised some concerns. As drafted, the policy will apply to "all devices, independent of their location or ownership, when connected to a UC network or cloud service used to store or process Institutional Information." It would be helpful to gain an understanding of the limits of the applicability of the policy for faculty, other employees, or campus guests who are using their personal electronic devices on the property of the University of California.

The Division suggests providing local campuses guidance on how roles that are assigned differing levels of security responsibility (e.g. Unit Head, Workforce Manager, Workforce Member, & Researchers) map to the traditional academia hierarchy (e.g. Deans, Department Chairs, Faculty, Principal Investigators, Postdoctoral Scholars, Graduate Students, and Undergraduate Students). We are concerned that the lack of clarity about the assigned roles may result in faculty unknowingly assuming security responsibilities. The policy also needs to be very specific about the type of violations that are deemed non-compliant, considering the serious consequences, outlined in *Section 1.2.1 - Violations and Sanctions* and *Section 1.2.2-Cost of Information Security Incident*, arising from "confirmed serious violations." It may be useful to create a plain-language policy summary that articulates the essential requirements for faculty and other employees to be in compliance with the policy.

The Santa Cruz Division is supportive of the different tiers of security and privacy, however, there was insufficient discussion on how this classification of information would occur. More direction on the type of security information that can be slotted into the different tiers of security and privacy would be useful.

Section 7.1-Human Resource Security: Prior to Employment, indicates that background checks will be required for personnel with access to Institutional Information classified at Protection Level 3 or higher

and for personnel with access to IT resources classified at Availability Level 3 or higher. The glossary specifies that data from large grants and identifiable human subjects will be classified at Protection levels 3 and 4, respectively, which implies that many faculty, teaching assistants, graduate students and undergraduate students would be subject to background checks. Information about what the background checks entail would be useful.

The Santa Cruz Division strongly recommends that the decisions about the classification of data into security tiers should remain with the Academic Senate and researchers, and this should be stated explicitly in the policy. Faculty are best positioned to weigh and balance the needs for privacy with those for open access, and the faculty professional associations provide ethical codes to guide these decisions. We believe it is critical that the Academic Senate continues to be involved in the evaluation, implementation, and consultation of future revisions.

Sincerely,

A handwritten signature in black ink, appearing to read 'Ólöf Einarsdóttir', written in a cursive style.

Ólöf Einarsdóttir, Chair
Academic Senate
Santa Cruz Division

cc: Thorne Lay, Chair, Committee on Academic Freedom
Brant Robertson, Chair, Committee on Information Technology
Eileen Zurbriggen, Chair, Committee on Library and Scholarly Communication

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 to 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,

A handwritten signature in black ink, appearing to read 'Ruth Greenblatt', written in a cursive style.

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

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 to 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 breaches, 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

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



UNIVERSITY COMMITTEE ON RESEARCH POLICY
(UCORP)
Isaac Martin, Chair
Email: iwmartin@ucsd.edu

University of California
Academic Senate
1111 Franklin Street, 12th Fl.
Oakland, California 94607

June 29, 2017

JAMES A. CHALFANT
CHAIR, ACADEMIC COUNCIL

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

Dear Jim,

The University Committee on Research Policy (UCORP) met on June 12, 2017, and discussed the Proposed Revised Presidential Policy on Electronic Information Security (IS-3). UCORP members take information security policy very seriously and have a number of concerns about the privacy implications of existing information security practices in the UC system. We were eager to have policy clarified. We were generally disappointed by the proposed revised policy, which we found did not clarify matters, and which raised several new concerns about the potential compliance implications for faculty.

The link to the “roles and responsibilities” on the Systemwide Information Security web site (<https://security.ucop.edu/guides/>) should be clearly indicated in the policy.

The roles and responsibilities themselves also appear to require further clarification.

One set of issues requiring clarification concerns the distinction between Unit Heads, who carry greater compliance and reporting responsibilities, and other Workforce Members. It was not clear to us when a faculty member should be understood to fall into one or the other of these categories. Although section II defines “Workforce Member” to include faculty, the same section also notes that principal investigators may be “Unit Heads” under some (unspecified) circumstances, and the example 3 under “Unit Head” in the attached Glossary is “A faculty member [who] is running a large research project under a federal grant that involves faculty at other universities.” In this example, the size of the research project, and the external grant funding, would seem to be red herrings; neither size of research project nor source of funding appears germane to the definition of a Unit Head. The conceptual criterion that a Unit Head is a person who has authority over IT resources could in principle implicate any faculty member who is empowered to purchase and install software. Yet the conceptual criterion that a Unit Head is equivalent to a dean in responsibility suggests a much smaller group of faculty have Unit Head responsibilities.

A second set of issues concerns the ambiguous locus of responsibility when faculty from different units collaborate. Interdisciplinary (and even cross-campus) collaboration is common in the UC system. If two co-PIs on a grant-funded research project, say, are in different units with different information security policies, whose information security procedures govern? The question might arise very often, for example, when health sciences faculty who collaborate with social science or engineering faculty. The members of UCORP could not find any guidance for such situations in the proposed policy. But guidance for such situations is precisely what we would hope for from a systemwide policy.

A third set of issues concern the implications of information security policy for faculty privacy and autonomy. Some UCORP members expressed concern over intrusive forms of monitoring. Others expressed concern for faculty autonomy in the face of the centralization of control over information technology resources—there is variability within the UC system, for example, in whether individual faculty members are permitted the necessary privileges to install software on their own laptops. The implications of UC information security policy for privacy and autonomy, in short, are of considerable interest, but we could not tell what the implications of the proposed revised policy were. It is at such a high level of abstraction that we struggled to discern any very clear connection between actual policy and practice on our campuses and the proposed revised policy.

Finally, UCORP members noted the general unclarity and disorganization of the proposed policy. There is one section of definitions in the proposed policy, and a glossary in an appendix to the proposed policy. They define many of the same terms but not in precisely the same way. Several definitions in the glossary include numbered lists, where the relationship between the items in the list is, presumably, either a logical “or,” as in the numbered items in a dictionary definition, or a logical “and,” but it is not clear which is intended, so the definition is unclear. Several important steps in the policy text use the term “and/or” in applications where the difference between “and” and “or” might be a big deal. For example, under III.2.3., the table entry for “standard” describes governance procedure, in part, as follows: “Provide an opportunity for the Academic Senate and/or UC Academic Computing Committee to appoint a member to the working group.” So is it to be the Senate as a whole, or UCACC, that appoints a member to the working group? Or both?

In summary, UCORP looks forward to reviewing a more clearly written draft proposed revised information security policy in academic year 2017-18.

Regards,



Isaac Martin
Chair, University Committee on Research Policy

cc: Shane White, Academic Council Vice Chair
Hilary Baxter, Academic Senate Director
UCORP Members



UNIVERSITY COMMITTEE ON FACULTY WELFARE (UCFW)
Lori Lubin, Chair
llubin@ucdavis.edu

Assembly of the Academic Senate
1111 Franklin Street, 12th
Oakland, CA 94607-5200
Phone: (510) 987-9466
Fax: (510) 763-0309

June 20, 2017

**JIM CHALFANT, CHAIR
ACADEMIC COUNCIL**

RE: Draft Revised Presidential Policy on Electronic Information Security (IS-3)

Dear Jim,

The University Committee on Faculty Welfare (UCFW) has discussed the Draft Revised Presidential Policy on Electronic Information Security (IS-3), and we find that the identified faults from the management review conducted earlier this year remain unaddressed. The policy remains inaccessible to end users, overly ambitious in scope for a single policy, silent on issues of inter-institutional research protocols, and does not highlight the need for resources to enable training and communications in this complex and rapidly changing area. In short, the committee cannot support the current draft, and we urge that further revision occur.

Thank you for your concern to this important topic. Our management review findings are enclosed.

Sincerely,

Lori Lubin, UCFW Chair

Encl.

Copy: UCFW
Hilary Baxter, Executive Director, Academic Senate



UNIVERSITY COMMITTEE ON FACULTY WELFARE (UCFW)
Lori Lubin, Chair
llubin@ucdavis.edu

Assembly of the Academic Senate
1111 Franklin Street, 12th
Oakland, CA 94607-5200
Phone: (510) 987-9466
Fax: (510) 763-0309

March 24, 2017

**JIM CHALFANT, CHAIR
ACADEMIC COUNCIL**

RE: Draft Revised Presidential Policy on Electronic Information Security (IS-3)

Dear Jim,

The University Committee on Faculty Welfare (UCFW) has discussed in management review the draft revised Presidential Policy on Electronic Information Security (IS-3), and we have several comments. While we agree that cybersecurity is an area in which the University needs to make significant strides forward, we think that this policy will not provide sufficient guidance to ensure the necessary progress. External threats, tighter federal regulations, and basic common sense demand improvements, but this policy seems too generic and abstract to be implemented. The verbiage and structure are reminiscent of a project management protocol for subject-matter experts; end-users will likely find this inaccessible and vague.

Internally, the structure of the proposed document could be improved. We understand that one goal is to establish a uniform framework for implementing cybersecurity without impairing the mission of the university, but given the size and scope of the University, this goal seems too ambitious for a single policy. We suggest instead developing specific policies for the general campus, for the health services, and for the national labs/classified projects. This structure would allow for greater clarity regarding different requirements.

Finally, we note that improving cybersecurity at UC will require significant on-the-ground resources and monitoring. The cooperation and support of local IT personnel will be critical, especially because members of the UC community use multiple electronic devices (including personal devices) with access to potentially sensitive information. The training and compliance demands imposed by so many devices and users should not be underestimated. Developing a system-wide 'clearinghouse' site that easily answer users' questions, and provides resources (drivers, malware detectors), for a wide range of devices and OSes, for example, might be an efficient approach to managing that problem.

Another specific concern not addressed by the document pertains to the diverse research environments of the UC system: faculty and other researchers share customized code with other researchers, and the proposed policy does not seem to anticipate that practice.

A final question is whether a three-year policy review horizon is too long given the rapidity of change in this area.

In summary, we find this draft in need of significant revision. It should better consider its intended audience and purpose, refine its scope to reduce its current cumbersomeness, and plan for needed resources and implementation. In closing, we also hope that UCOP will allocate the resources required to allow the implementation of effective cybersecurity policies.

Sincerely,

Lori Lubin, UCFW Chair

Copy: UCFW
Hilary Baxter, Executive Director, Academic Senate



UNIVERSITY COMMITTEE ON PLANNING AND BUDGET (UCPB)
Bernard Sadoulet, Chair
sadoulet@berkeley.edu

Assembly of the Academic Senate
1111 Franklin Street, 12th Floor
Oakland, CA 94607-5200
Phone: (510) 987-9466
Fax: (510) 763-0309

July 21, 2017

**JIM CHALFANT, CHAIR
ACADEMIC COUNCIL**

RE: Proposed Revised Presidential Policy on Electronic Information Security

Dear Jim,

The University Committee on Planning and Budget (UCPB) has discussed the proposed revised Presidential Policy on Electronic Information Security (IS-3), and we have several concerns with the proposal. Overall, we find the proposal to be simultaneously too vague and too technical. It is vague in the sense that its goals are poorly articulated, and no guidance is included for end users, other than the too technical specifications which only make sense to IS professionals. The proposal shifts an undue amount of responsibility onto end-users – again absent meaningful guidance – and in addition to the already precipitate loss in staff support incurred by most faculty. Indeed, statements such as “All Workforce Members are responsible for ensuring the protection of Institutional Information and IT Resources”, by themselves, are at best a fig leaf for the administration. Without safety nets, tools and clear processes (and fences), faculty and researchers are left exposed. The crux of achieving information security in the UC will be the development and deployment of such safety nets, tools, etc. Moreover, consistency across the campuses will also be necessary, and collaborations with researchers at other institutions must also be addressed.

In short, adopting the present draft policy by itself at this stage makes a lot of people non-compliant, but does not actually improve security. Further, we cannot adopt – at least, not in any meaningful way – a policy that we cannot implement.

We enclose some of the specific feedback we received in hopes that it will guide subsequent revision of a more viable policy.

Sincerely,

Bernard Sadoulet, Chair
UCPB

cc: UCPB
Hilary Baxter, Executive Director, Systemwide Academic Senate

Comment: “Rather than telling me that it is my responsibility never to have my password phished, you should set systems up in a way that even if my password were phished, it would not be sufficient to gain access. Rather than mandate antivirus and tell me it is my responsibility never to run malware that slips by it, you should ask me to access sensitive information from a computer that resists any but the most sophisticated attackers.”

Further: “Nothing in the [proposed policy] will make UC meaningfully more secure; at best it would shift liability to end users: ‘we mandated best practices, but you still got phished!’ Perhaps that’s how the policy is intended, given the line, ‘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.’” (This comment is echoed by another comment, below.)

Comment: At a high level, this policy achieves a lot of the right things. It identifies risk levels, responsible individuals, SLAs, the need for risk-cost-benefit analysis, and accountability. Having said that, there are some narrow areas that concern me in what is written – and some big areas with respect to what isn’t written.

An example “narrow area”: Better guidance is probably needed on the division between P3 and P4. At a high level, P4 is the “long term institutional impact big stuff” and P3 is the “a mess for a while institutional impact big stuff”, but that is sometimes hard to distinguish in advance other than by a lot of brainstorming about impact from those at the top. This brainstorming can probably happen and be documented in advance, institutionally, at least for much of it.

Another concern: Things that might be P2 or below can become P3 if the basket becomes large enough for the aggregate exposure to be large enough. Such would make sense from a risk perspective. But, the mechanisms are going to have a really hard time supporting it. Unless a human notices and voluntarily uses the higher classification, the mechanisms will likely steer the process toward the one used by the lower classification. It is hard to support good decision-making when the mechanisms are steering the wrong way.

Comment: A bigger concern is with what isn’t written. How is an end user or developer to implement this? What are the mechanisms? How are they assembled into a process?

For example, what encrypted container do I use? How does it get installed? What happens to it when I go on sabbatical or leave the university? What if it is on personal equipment? Who keeps it up to date with respect to security updates? How is the environment around it protected from malware so my password to the encrypted volume isn’t snatched?

Let’s assume that is now done. How does my protected data get into the volume? When I download things, the encrypted volume probably isn’t the default destination. So, human error will put things in other places. I might then move these things – but the original isn’t likely to be deleted, never mind overwritten. What policy governs the security for this container? How long can a session be active without needing to be refreshed? Can my password be in a keychain? Or, does it need to be 2-factor? Can I write it down? What if there are too many passwords for a human to remember? Or different biometric systems in place from one system hosting the container to another? What protections should be in place should I try to export from this container? For example, copying data out of it? Or printing data out of it? Or printing data to a .pdf file saved outside of it?

What about data that is currently presented to user in plain text? When I download student records, they come in .csv files! I’ll bet financial records do, too. Is it my problem to encrypt them and/or get them into

an encrypted container? What about after a download and before a move (if I download to the wrong place), do I have to delete the data? Overwrite it? How? Do we really expect compliance with that?

Why not rewrite the apps so that downloads happen via encrypted .pdf file or .zip files, etc? That way I get them in a safe way. It is an interesting question as to whether or not to use an existing password for this purpose, so humans don't get overloaded, or a per-session password for maximum safety.

Whenever the tool chain is developed, how does the user get it? And, what about the local policy settings to automate it, e.g., reset default download directory. Do we have a way to do this for, at least, OS X, Windows, and Linux? Or, can we put together a standardized VM that can be used for this purpose, so users can just get one ball? How is it kept up to date?

What are the key usage cases? The policy document is silent on this. We really need these for those big classes of users impacted: teachers, researchers, academic support, various financial users and managers. Without these, we won't know if the proposed workflow works. Please give more details of the validations and sanity-checking of the policy *against concrete use cases and usage scenarios*.