



Chair, Academic Council and Assembly of the Academic Senate
Telephone: (510) 987-9303
Fax: (510) 763-0309
Email: John.Oakley@ucop.edu

Faculty Representative to the Board of Regents
University of California
1111 Franklin Street, 12th Floor
Oakland, California 94607-5200

March 8, 2007

**KRISTINE A. HAFNER, ASSOCIATE VICE PRESIDENT
INFORMATION RESOURCES AND COMMUNICATIONS**

**Re: Academic Senate Review of the Proposed Presidential Policy and Guidelines on
Stewardship of Electronic Information Resources**

Dear Kris,

I am pleased to report the outcome of the Academic Senate's formal review of the proposed *Presidential Policy and Guidelines on Stewardship of Electronic Information Resources*. After careful consideration, the Academic Council approves of the proposed policy given that first, the issues and recommendations highlighted below (and provided in their entirety in the attached letters from participating Senate reviewers) are afforded careful consideration, and second, the Academic Council is given the opportunity to review and comment on a revised policy prior to its final issuance by President Dynes.

Support as Written (Information Technology and Telecommunications Policy Committee (ITTP))

- UC's efforts to maintain and protect the important data targeted by this policy are vital to the security of the institution and its personnel. The policy primarily serves as a guide to the campuses, and thus is targeted appropriately at campus IT managers with an appropriate level of detail, content, and assumed familiarity with terminology and policy (ITTP).
- **Comments on Policy Dissemination and Implementation:** ITTP provides a list of specific steps that should follow adoption of the policy, and guide implementation, including role-specific policy documentation, directions, and training, which would be appropriately developed at the systemwide level.

Support, With Need for Clarification/Addition (University Committee on Library (UCOL), Berkeley, Davis, Los Angeles, Riverside, San Francisco, Santa Barbara)

- Clearly define the following terminology, which is sometimes used synonymously in the policy: stewardship, scholarly information, academic information, electronic information systems, electronic information, university information, institutional information, departmental information, and major enterprise systems (UCOL; with additional suggestions from Riverside). Without knowledge of all elements of electronic information, for example, oversight of the stewardship effort will surely fail (San

Francisco). Stewardship may be commonly known as long term commitment to maintenance, but that clearly is not the goal of this policy (Santa Barbara).

- Clarify which kinds departmental information will be subject to this policy (UCOL).
- Policy should outline alternate security policies for non-network based systems [Sections 4 and 5] (Davis).
- Clarify how this policy conforms with the University's default principle of openness of information (Los Angeles).
- Need to build-in flexibility for levels of protection required for different kinds of data (Los Angeles).
- The "Identity and Access Management" section should be altered to allow for confirmation of people who do not have a government-issued ID, such as altering the policy to adopt a tiered identity structure such as that used at UCLA (Los Angeles).
- Policy should clearly state how to dispose of electronic information devices that are no longer needed but contain sensitive data (Los Angeles).
- Clarify how and by whom the "identification and prohibition of software posing security risks" will be accomplished (Riverside, Santa Barbara).
- Allow for the preservation of Common Architecture when appropriate (Riverside).
- Add discussion about the interaction between administration and academic enterprises, and the coordination of activities across these enterprises (San Francisco).
- Implement standardized risk reduction practices across the University, such as minimum specific locking mechanisms for laptops, specific encryption techniques, and required updating of access accounts on a defined schedule. Also clarify the disparities between high and low level risk (San Francisco).
- Clarify the meaning of the statement that "campuses should ensure that purchases of technology-based high-value goods and services receive appropriate review," so as to avoid adopting a highly restrictive model with the potential to inhibit researchers (Santa Barbara).

Other Issues

- **Unfunded Mandate:** Policy could appear to be an unfunded mandate on the campuses. Policy places a strain on both financial and technical support resources (Berkeley, Davis, San Francisco).
 - **Recommendations:** The University could ease implementation by providing security software repositories for all users to easily access software license information, instructions, updates, etc. (Davis). And the policy should state that the University and/or the campuses must ensure that University members have the resources to achieve compliance, and that the members must institute the appropriate measures when given those resources (San Francisco).
- **Burdensome Technical Requirements:** Terms such as "encrypted authorization," and "authenticated email relay" are not catch-alls and are too specific [Section 4B]. The policy should instead focus on what is to be done, and less on how it is to be done (Davis).
- **Language of IT Professionals:** how can all members of the University community be held accountable for stewardship when unfamiliar with IT language and policy? (Santa Barbara)

- Suggestion that the ITTP Chair be appointed to serve as the *ex officio* Senate representative to the Information Technology Leadership Council (Los Angeles).

Explicit Opposition Unless Policy is Re-Drafted (UCEP, Irvine)

Need for Clarification/Addition (Please see comment letters for more detail)

- What kind of data does the policy cover?
- What specific measures will be required of faculty to protect the covered information?
- Who determines the appropriate software and compliance procedures?
- What are the consequences of unwittingly violating the policy?
- How will those responsible for sensitive information be trained?

Specific Recommendations (Please see Irvine letter for more detail)

- Provide specific guidelines for faculty.
- Define and disseminate best practices for protecting information.
- Delete “removal of unnecessary services” from Section 4B because such authority is too far-reaching and ill-defined.

Ensuring the security of the University’s data and information is a worthy and necessary goal that we all wish to accomplish. On behalf of the Academic Council, I applaud the spirit of the proposed *Presidential Policy and Guidelines on Stewardship of Electronic Information Resources*, and look forward to the receipt of another draft of this policy for the Council’s review. Please contact me if you foresee any problems with this request.

Sincerely,



John B. Oakley, Chair
Academic Council

Copy: Academic Council
María Bertero-Barceló, Executive Director

Enclosures: 10

JO/MAR



INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS POLICY
David Messerschmitt, Chair
messer@eecs.berkeley.edu

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

November 17, 2006

**JOHN OAKLEY, CHAIR
ACADEMIC SENATE**

RE: Proposed Policy on Stewardship of Electronic Information, out for Senate-wide review

Dear John,

At its November 9, 2006 meeting, the University Committee on Information Technology and Telecommunications Policy (ITTP) discussed the proposed Policy on Stewardship of Electronic Information. ITTP recognizes that enhancing UC's efforts to maintain and protect the important data targeted by this Policy is vital to the security of the institution and its personnel, and we applaud these efforts. We understand that the Policy is intended to guide the campuses, and thus it is targeted first and foremost at IT managers on the various campuses—those responsible for information security policy and planning. It serves this goal well. It is at an appropriate level of detail and uses terminology that these managers will comprehend.

While we enthusiastically support the purpose of the proposed Policy and endorse it, I would like to bring to your attention some concerns regarding the future dissemination and implementation of the guidelines.

Successful information security requires active training for all employees who possess or have access to sensitive information. Technology alone, or actions or policies on the part of campus IT leadership, will not provide sufficient protection to this data because individual users can always compromise data security through mistakes or inattention. Moreover, the Policy itself will likely not be read or understood by a wide cross-section of users because of its length and use of unfamiliar terminology. Finally, as a policy, it appropriately does not give specific how-to directions to guide the day-to-day actions of users. Thus, it is important that the Policy be followed by additional, specific steps, such as providing:

- Role-specific policy documentation (e.g. for course instructors, for human subject researchers, for departmental administrators, etc.) that presents the users' responsibilities in the context of their specific needs and in terminology familiar to them.
- Role-specific how-to directions for completing the tasks necessary to fulfill each user's technical responsibilities, such as encryption, backup, computer security measures, etc.
- Role-specific training, especially for those with responsibility for particularly sensitive data.

The Policy addresses areas of such vital importance to the University in fulfilling its responsibilities to students, human research subjects, and others, that we also believe role-based training should be *required* in some cases. It would also be appropriate to require, in advance, a written plan for data protection and

incident follow-up in particularly sensitive cases. In other cases, it may be sufficient to notify employees of their responsibilities and provide the necessary documentation through supervisors, academic deans, etc.

There is sufficient commonality in these needs that we believe it would be sufficient and appropriate to develop documentation and training materials on a systemwide-basis, or at one campus followed by systemwide promulgation, rather than duplicate this effort across the University's ten campuses.

Regardless of how IR&C chooses to address these issues, the first step is to approve the Policy. Again, ITTP endorses the proposed Policy, and looks forward to its thoughtful implementation.

Sincerely,

David Messerschmitt, Chair
ITTP

cc: Maria Bertero-Barcelo, Executive Director
ITTP



UNIVERSITY COMMITTEE ON EDUCATIONAL POLICY (UCEP)
RICHARD WEISS, CHAIR
weiss@chem.ucla.edu

The Academic Council
1111 Franklin Street, 12th Floor
Oakland, CA 94607-5200
Phone: (510) 987-9467
Fax: (510) 763-0309

December 4, 2006

JOHN OAKLEY, CHAIR
ACADEMIC COUNCIL

Re: Proposed Policy on Stewardship of Electronic Information

Dear John,

In November, the University Committee on Educational Policy (UCEP) reviewed the proposed Systemwide Policy on Stewardship of Electronic Information. Unfortunately we feel the policy leaves too many questions unanswered, and as a result, we are unable to endorse it at this time. The document should provide clearer, more precise guidance about what legal responsibilities and obligations the faculty would have for protecting student information under the new guidelines.

The following points summarize the questions and concerns identified by UCEP members:

➤ *What kind of data does the policy cover?*

Nearly every instructor keeps information about students on a computer, including grades, letters of recommendation, and e-mail correspondence. But precisely what kind of information is covered by the policy—student names? Grades? Test and Assignment Scores? ID numbers? E-mail addresses? Phone numbers? Mailing addresses? Social Security numbers?

➤ *What specific measures will be required of faculty to protect the covered information?*

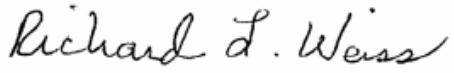
Will faculty be required to encrypt data, or is a password-protected login sufficient? Should faculty lock desktop and laptop computers to a desk, or is a locked office acceptable? What if the instructor steps away from the office momentarily? What about external hard disk drives?

➤ *Who determines the appropriate software and compliance procedures?*

Will campuses entities or individual faculty be asked to invest in the added software or computer support necessary to comply with the policy? Will equivalent software and procedures be available for every kind of computer (not just those using Windows)? What if an expensive overhaul is required to modernize older systems?

UCEP agrees that protecting the privacy of students is important, but those protections should also be balanced with sensible considerations of cost, convenience, and the instructor's ability to work effectively. The proposed policy is well-intentioned, but as currently formulated it is far too ambiguous and seems to have been written without much understanding of its practical effects.

Sincerely,

A handwritten signature in cursive script that reads "Richard L. Weiss". The signature is written in black ink on a light gray background.

Richard Weiss
Chair, UCEP

cc: UCEP members
Executive Director Bertero-Barceló



UNIVERSITY COMMITTEE ON LIBRARY (UCOL)
Ben Crow, Chair
bencrow@ucsc.edu

The Assembly of the
Academic Senate
1111 Franklin Street, 12th Floor
Oakland, CA 94607-5200
Phone: (510) 587-6138
Fax: (510) 763-0309

December 1, 2006

JOHN OAKLEY, CHAIR
ACADEMIC COUNCIL

RE: Proposed Policy on Stewardship of Electronic Information

Dear John,

At its last meeting, UCOL reviewed the proposed policy on Stewardship of Electronic Information. While members generally agreed that the proposed policy was sound and thorough, they pointed out that 'stewardship' carries a number of meanings and connotations. For example, within scholarly communication 'stewardship' typically denotes the preservation of scholarly materials in digital format.

Along these same lines, members remarked that the proposal uses a number of terms synonymously. This terminology includes: scholarly information, academic information, electronic information systems, electronic information, university information, institutional information, departmental information, and major enterprise systems. Members asked that the proposal make a distinction between these terms, or at least define them more precisely. The committee also inquired if some or all of these terms are considered key technical terms in the field of information technology.

Finally, members wanted to know if all departmental information would be subject to this policy. If not, then the proposal should distinguish between the kinds of departmental information that would be subject to the policy, and which kinds of departmental information that would not. If you have any questions, please let me know.

Respectfully submitted,

A handwritten signature in dark ink, appearing to read "Ben Crow". The signature is fluid and cursive, with the first name "Ben" and last name "Crow" clearly distinguishable.

Ben Crow
Chair, UCOL

cc: UCOL
Executive Director Bertero-Barcelo



February 16, 2007

JOHN OAKLEY
Chair, Academic Senate

Subject: Proposed policy on stewardship of electronic information resources

On February 12, 2007, the Divisional Council (DIVCO) of the Berkeley Division discussed the proposed policy cited above, along with the comments of the divisional Committee on Computing and Communications. DIVCO noted that the proposed policy is not concrete, and procedures for implementation are not defined. This allows campuses flexibility to tailor policies to their own individual circumstances, but also raises issues of oversight for divisions of the Senate.

DIVCO also cautioned against the imposition of unfunded mandates. For example, the requirement that encryption measures be employed and implemented could necessitate the purchase of new hardware, such as laptops and PDA's. The proposed policy is mute on how such provisions will be funded.

Sincerely,

A handwritten signature in black ink, appearing to read 'William Drummond', on a light-colored background.

William Drummond
Chair, Berkeley Division of the Academic Senate

Cc: Martin Head-Gordon, Chair, Committee on Computing and Communications
Margarita Zeglin, Committee on Computing and Communications staff



OFFICE OF THE ACADEMIC SENATE
ONE SHIELDS AVENUE
DAVIS, CALIFORNIA 95616-8502
TELEPHONE: (530) 752-2231

January 8, 2006

John Oakley, Chair

Assembly of the Academic Senate
Academic Council
1111 Franklin Street, 12th Floor
Oakland, CA 94607-5200

Re: System-wide Review of the Proposed Policy on Stewardship of Electronic Information

In general, the policy appears to be written by and for experts in information technology. We strongly endorse the effort to protect electronic information and the privacy of members of the university community. However, a major effect of the proposed policy seems to be to transfer liability from the institution and to devolve responsibility for information security to smaller units and individuals who may not have the technical expertise or knowledge either to understand the meaning and implications of the policy or to carry out the necessary protections.

The proposal does not address how campuses are to support implementation of the standard. In the past, the technique used might be termed an “unfunded mandate”. The campus simply requires administrative units to comply with requirements, without providing any financial or technical support. This means that administrative units with limited computer support and/or staff must choose between trying to ensure compliance with this policy, and trying to do the work necessary to support the academic mission. What may well happen is that units will report compliance with the policy, not realizing they are not complying; or units will report that they cannot comply with the policy unless the campus gives support. While the policy cannot prevent this, it should point out the need for campuses to provide support for administrative units that lack enough resources or people to both carry out their academic mission and ensure compliance with this policy.

The university could offer assistance by providing campus or systemwide repositories of security software. For example, currently, each department or individual user must procure their own copy of an antivirus program, install it, configure it, and maintain it (including applying patches). If each campus, or the UC system, had a site or system license for the software, made it easily available, provided detailed instructions on how to install, configure, and update it, and made updates available, then the software becomes more attractive for, and accessible to, members of the campus community.

Section 4 focuses on network access. In particular, section 4B states that “[e]ach campus must establish minimum standards for devices connected to their networks ...”, implying that if a system is not connected to the network, there need not be *any* standard for security that the system must meet. A similar

observation holds for section 5. In that section, “authentication” is defined as confirming identity by verifying digital credentials enabling the user to access a network-based service, and “authorization” is defined in terms of permitting access to network-based services. This implies that if a system or service is *not* network-based, then the requirements of that section do not apply. If intended, this is very bad because it allows anyone to walk up to a system and access it, even if that system contains information that should be protected. If not intended, the definitions should be rephrased to apply to network-based and non-network-based systems alike.

Finally, the technical requirements often focus on mechanism rather than goals. In particular, section 4B requires several security mechanisms be addressed by campus standards. Encrypted authentication, for example, is unnecessary on many systems; a challenge-response mechanism involving random numbers does not require encrypted passwords and works equally well. It would be better to write this as “protecting authentication information”, which includes enciphering reusable passwords being sent over a network. An “authenticated email relay” is unclear; do you mean the server authenticates to the client, or the client to the server? Also, there are other techniques that prevent mail relay, so perhaps a more general term such as “preventing unauthorized mail relaying” would be a better way to phrase this. In general, the policy should focus on what is to be done, and less on how it is to be done.

Sincerely,

Linda F. Bisson
Professor of Viticulture & Enology
Chair of the Davis Division of the Academic Senate



Office of the Academic Senate
2300 Berkeley Place South
Irvine, CA 92697-1325
(949) 824-2215 FAX

December 7, 2006

John Oakley, Chair, Academic Council
1111 Franklin Street, 12th Floor
Oakland, CA 94607-5200

RE: Proposed Policy on Stewardship of Electronic Information

Several Councils and the Senate Cabinet of the Irvine Divisional Senate reviewed the proposed principles and agreed that these revisions to the policy are well-intentioned but lacking in adequate guidance and detail, overly broad, and overlapping with existing or planned policies. We believe that the UC Information Security Work Group should re-draft the proposal. We hope that the following questions in Section I and the recommendations in Section II will be helpful.

I. Questions:

- A. Precisely what kind of information is covered?
 - 1. Student names?
 - 2. Student grades?
 - 3. Scores on assignments?
 - 4. Electronic mail messages and other private correspondence?
 - 5. Student ID numbers?
 - 6. Students' e-mail addresses?
 - 7. Phone numbers?
 - 8. Mailing addresses?
 - 9. Social Security numbers?
- B. What measures do faculty have to take to protect the covered information?
 - 1. Do faculty have to encrypt the data on their hard drive, or is it enough to require a password to log in?
 - 2. Must faculty keep their desktop computer physically locked to a desk, or is a locked office acceptable?
 - 3. What measures are required for laptop computers or external hard disk drives?
 - 4. For how long is it permissible to leave a computer unsecured (e.g., a laptop in a briefcase)? May it be left unattended momentarily?
 - 5. Who will determine what software or procedures are sufficient for compliance? Who will make sure that equivalent procedures are available on every kind of computer (not just Windows machines)? And, who will pay for any necessary software or computer support to set these up, or for modernizing systems that are too old to comply?
- C. Would adoption of the new policy and guidelines, given the lack of important implementation details, place numerous UCI employees in unwitting violation of the

policies and guidelines? For example, what are the policies for storing merit and promotion recommendations?

- D. How will those responsible for maintaining sensitive electronic information learn the security and legal risks and best practices for storing the information?
- E. Removal of “unnecessary services” (4B) goes against the spirit of research and exploration and against common sense. Who is to decide what services are unnecessary or what the intended purpose or operation of information technology devices is? And how would this be transparent to everyone? Surely there would be a large opportunity cost in content and hardware development if the policy succeeded in locking down systems.

II. Recommendations:

- A. The guidelines should be condensed, with much of the document relying on references to existing policies that already address the issues discussed.
- B. The resulting document should put existing or planned security, records retention, identity management, disaster recovery, and other policies into the context of data stewardship.
- C. The proposed policy needs to be explicit about what kinds of data are protected, what measures are adequate to protect it, and who is responsible for installing, maintaining, supporting, and financing those measures.
- D. There should be specific guidelines for faculty. Instructors need clear-cut guidance about what their responsibilities are.
- E. The best methods for protecting information should be explicitly defined and disseminated for the most widespread practices.
- F. Since faculty are accountable for violations of the Faculty Code of Conduct, which does not address the handling of electronic information, the Faculty Code of Conduct may need to be modified to ensure accountability in the case of faculty failure to safeguard electronic information.
- G. In 4B, delete the bullet point regarding “removal of unnecessary services.” Such a far-reaching and ill-defined authority to suppress information technology would run counter to the overall aims of the policy.

Irvine acknowledges the importance of protecting privacy and the integrity of University information, but how we do it has to be clearly defined and balanced with cost and convenience and an instructor's ability to work effectively.

A handwritten signature in dark ink, reading "Martha McCartney". The signature is fluid and cursive, with a large loop at the end of the last name.

Martha McCartney, Senate Chair



ACADEMIC SENATE EXECUTIVE OFFICE
LOS ANGELES DIVISION
3125 MURPHY HALL
LOS ANGELES, CA 90095-1408

PHONE: (310) 825-3851
FAX: (310) 206-5273

January 11, 2007

Professor John Oakley
Chair of the Academic Council
1111 Franklin Street, 12th Floor
Oakland, CA 94607

In Re: Proposed Policy on Stewardship of Electronic Information

Dear John:

Thank you for the opportunity to review and opine upon the Proposed Policy on Stewardship of Electronic Information. Please extend my gratitude to the faculty and staff who have no doubt given the proposal much consideration, planning, and effort. Upon receipt of the request for review, I invited all standing committees of the Academic Senate to opine. Additionally, I specifically requested that the following Senate Committees opine: Executive Board, Committee on Library (COL), and the Council on Planning and Budget (CPB). I also invited the joint Senate-Administration Information Technology Planning Board (ITPB) to opine. I am also pleased to report that UCLA's Advisory Board on Privacy and Data Protection (ABPDP), the Committee of IT Infrastructure (CITI) and the Common Systems Group (CSG—IT Directors from academic and administrative units around the campus) also took the initiative to opine—their response are included in ITPB's memo. Generally, the responses were positive; both the CPB and COL endorsed the proposal. However, as evidenced by the responses of the other senate committees, the UCLA Division has certain reservations:

- The Information Technology Leadership Council appointed by Chancellors, Medical Center Directors, and UC managed National Laboratories has no Academic Senate Representative. It urges that a Senate Member be appointed *ex officio* to the Council, and recommends that the Chair of the Systemwide Information Technology and Telecommunications Policy Committee serve in such a capacity. (Executive Board)
- The new guidelines are not properly framed with respect to the University's principle of openness of information. "University research and scholarship relies on open sharing of information and ideas; it is a principle that has stood the test of time and is essential for sound scholarly work. UCLA wants to ensure that the guidelines cannot be misinterpreted to mean that all electronic information need be secured for limited access. Ideally, the guidelines should make clear that openness prevails as the default unless a good reason for limited access exists, for example SB1386, HIPPA or FERPA data requirements." (ITBP, ABPDP, CITI, CSG)
- The proposal states, in passing, that measures taken to protect data should vary with circumstance. However, the overall implication of the guidelines is that all data must have

the same level of protection. “Certainly, this is not the case. While all data should be secured to maintain integrity, all data need not be secured for limited access or availability; in fact, quite the opposite. It should be possible to make data easily available and accessible for sharing information and ideas unless there is a good reason to limit access. Increasingly, funding agencies are making such access a requirement.” (ITPB, ABPDP, CITI, CSG)

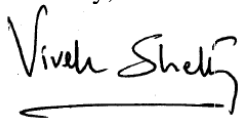
- The Identity and Access Management section, under subsection Identification, states that, “The identity of individuals must be confirmed by their presentation of valid current government issued photo ID to the campus unit that manages electronic identity information and that provides identity information and authentication services for their campuses.” UCLA’s primary difficulty with this statement is that there can be many types of users in an open University community, many of which will never have produced a photo ID.

UCLA currently handles this issue with a three-tiered identity management system whereby UCLA’s Enterprise Directory utilizes an Identity Trust Level attribute to define a user as Un-Verified, Normal or Physically Verified. Un-Verified identities are used as placeholder records for the temporary self-service guest accounts created in low security, pseudo-anonymous scenarios; examples of these are temporary conference material access and library research access. Normal identities are created by an authorized administrator or provisioned automatically using book-of-records data; examples of these are employees, students, contractors, and visiting scholars requiring ongoing access to UCLA resources. Physically Verified individuals are those whose identity has been confirmed by presentation of a valid current government issued photo ID; examples of these are faculty and staff who have presented photo ID to an authorized UCLA security administrator. UCLA recommends that the guidelines be altered to adopt a tiered identity structure. (ITPB, ABPDP, CITI, CSG)

- The proposal should address the disposition of electronic information devices that are no longer needed but contained sensitive data. (Reformatting disk drives or simply deleting files does not remove the sensitive data. Forensic capabilities to resurrect deleted files are readily available.) UCLA recommends that the policy require that devices should either be physically destroyed or wiped by overwriting each bit. The guidelines should clearly state how to dispose of such devices. (ITPB, ABPDP, CITI, CSG).

Thank you for your time and efforts. I hope our collective divisional insights are helpful in improving the Proposed Policy on Stewardship of Electronic Information.

Sincerely,



Vivek Shetty
Chair, UCLA Academic Senate

Cc: Maria Bertero-Barcelo, Executive Director of the Systemwide Senate
Jaime R. Balboa, Chief Administrative Officer of the UCLA Academic Senate



CHAIR, ACADEMIC SENATE
RIVERSIDE DIVISION
UNIVERSITY COLLEGE BUILDING
ROOM 225
TEL: (951) 827-5530
FAX: (951) 827-5545
SENATE@UCR.EDU

THOMAS COGSWELL
PROFESSOR OF HISTORY
RIVERSIDE, CA 92521-0217
TEL: (951) 827-1997
E-MAIL: THOMAS.COGSWELL@UCR.EDU

December 5, 2006

John Oakley
Professor of Law
Chair, UC Systemwide Academic Senate
1111 Franklin St., 12th Floor
Oakland, CA 94607

Dear John:

RE: REVIEW OF PROPOSED POLICY ON STEWARDSHIP OF ELECTRONIC INFORMATION

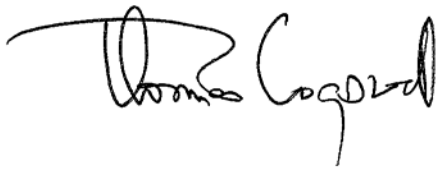
The proposed UC Policy on Stewardship of Electronic Information has been reviewed by our committee on Academic Computing and Information Technology, and they had no specific objections to the proposed policies per se. Nevertheless the committee felt the following points needed to be addressed:

- The Senate should prepare a layperson's guide, explaining in simple terms, how UC safeguards personal information and how individual students, staff and faculty may reduce the risk of information theft through simple actions such as changing passwords regularly etc. This pamphlet might be passed to MSO's, all student employees and faculty/staff, or maybe published as a webpage within the info security's pages or by each campus's office of computing and communications.
- This guide should also clarify whether the policy applies only to University generated data or whether it also refers to commercially produced/licensed information resources other than RMS (Resources Management Systems), such as licensed library type databases that fall under copyright and contract law.
- It would be useful to have a glossary of terminology and concepts to better understand the intent and scope of the draft policy, especially for such terms as:
 - University information assets (p.4)
 - Information resources, major enterprise systems, third party agreements (p.5)
 - Network-based service (p.7)
 - Online services (p.7)
 - Significant liability or other legal exposure (in relation to what kinds of information sources (p.8)
 - Technology-based high-value goods and services (p.9) o Electronic Information Resources (very, very broad) (p.9)
- It is vitally important that definitions of these key terms/concepts should be made clear so that those outside the field can fully understand the scope of the policy.

- The guide should include a section concerning the rights of individuals using University computing resources, including their privacy rights and freedom-from-censorship rights, e.g., the rights of art makers to be free of issues of censorship in university-created archives.
- Furthermore the section on identification and prohibition of software posing security risks raised some concerns as to how and by whom these would be accomplished and enforced. Prohibiting software use is a complicated issue in a research university - a more complex security model might be explored in cases where unprotected computing is desired.
- Finally, the section on Common Architecture raised some concerns. Historically, diversity of architectures has been strength of computing within the UC system and has led to significant innovation. For example, at a time when there was a push to standardize on IBM mainframes, Berkeley was developing and adopting UNIX and UCSD was experimenting with desktop computing.
- That diversity of architectures reflects the diversity of purposes to which computing is put within this system. While the economies of scale are well documented, there can be and have been severe (even scandalous) diseconomies in uniformity and in exclusive purchase contracts within this system.

With all best wishes, I remain,

Yours faithfully,

A handwritten signature in black ink, appearing to read "Thomas Cogswell". The signature is fluid and cursive, with a large initial "T" and a long, sweeping underline.

Thomas Cogswell
Professor of History:
and Chair of the Academic Senate
University of California
Riverside 92521



The Task Force Reviewing and Recommending Comment to the Proposed Policy on Stewardship of Electronic Information

David Teitel, MD, Chair

December 1, 2006

Deborah Greenspan, DSc, BDS
Chair, UCSF Academic Senate
Office of the Academic Senate, Box 0764

Dear Chair Greenspan,

The Task Force Reviewing and Recommending Comment to the Proposed Policy on Stewardship of Electronic Information, consisting of one member from the Committee on Library (to serve as Chair), one member from the Committee on Educational Policy, one member from the Committee on Academic Planning and Budget, one Member from the Clinical Affairs, the UCSF Representative to the systemwide Information Technology and Telecommunications Policy Committee (ITTP)*, and the Office of Academic and Administrative Information Systems (OAAIS)* Director of Enterprise Information Security, corresponded over email to review these recommendations and to suggest a possible response from the San Francisco Division. An addendum, prepared by Enterprise Information Security, gives an overview of the Stewardship Policy from the University of California Office of the President (UCOP)* and is attached [here](#).

1. The concept of endorsing practices that uphold the principles of privacy and confidentiality, integrity and timely access to information is laudable, and it is also essential to protect electronic resources, but the policy statement continues with "All members of the University community are accountable for compliance." Members may be accountable for their own actions but it is often outside their abilities to ensure compliance. Many entities on campus, while ready to comply with regulations such as HIPAA, are still without the necessary resources to achieve that compliance. It is unacceptable to produce a document requiring member accountability and not give the members the ability to comply. There is nothing in the document which addresses this critical issue. It should be stated that the University and/or campuses must ensure that the members have the resources to achieve compliance, and that the members must institute the appropriate measures when given those resources.

2. There is no discussion about the interaction between Administration and Academic enterprises, and, in the case of health science campuses, Clinical enterprises, to ensure adequate sharing and

*The original Communication from the Task Force was modified by the Coordinating Committee on December 12, 2006, to expand these acronyms to their full names.

protection of information. Coordinated activities across these enterprises should be encouraged at the University level. There is no single “secure technical environment” at the campuses, so that integration among them is essential. OAAIS is an example of such an interaction at UCSF.

3. Risk reduction should be achieved by measures standardized across the University, measures which should be re-evaluated and disseminated on a well-defined, regular basis. For example, minimum specific locking mechanisms and their maintenance for University laptop and other portable devices could be defined across campuses, to ensure that there is a minimum risk reduction achieved at all campuses. Specifying encryption techniques is another example of standardizing risk reduction. Updating access accounts on a defined schedule is another.

4. There is no discussion as to the oversight of the stewardship effort. Without knowledge of all elements of electronic information storage and utilization down to the individual user, how can any department or unit ensure compliance? The document should present a clear algorithm to define the scope of electronic information at each campus prior to requiring that some body function as its steward.

5. The document puts enormous responsibility on the individual campuses to undertake the entire effort, and only demands that the University writes this document. Further, there is a great deal of variation in the resources (human, technology, financial, knowledge) across the specific institutions that this document will cover and for some institutions this may be a minor burden whereas for many of the institutions this require a significant expenditure in resources to support compliance with this policy. This is likely to result in a spotty or incomplete application of this policy. The Information Technology Leadership Council could have resources to offer far greater support of the individual campuses activities, to minimize duplication of effort.

6. Lastly, this policy does not address the disparities between low level and high level risk for electronic information and sets too high of expectations for information that carries a low/no level risk.

The Task Force thanks you for the opportunity to review and comment on this report. Should you have any questions, please do not hesitate to ask.

Sincerely,

Task Force Reviewing and Recommending Comment to the Proposed Policy on Stewardship of Electronic Information

Task Force Membership

David Teitel, MD, Committee on Library, Chair of the Task Force

William Bird, DDS, DrPh, Committee on Educational Policy

Steven Cheung, MD, Academic Planning and Budget

Mary Lynch, RN, MS, MPH, PNP, Clinical Affairs Committee

Donna Hudson, PhD, UCSF Representative to UC Information Technology and Telecommunications Policy Committee

Carl Tianen, OAAIS Director of Enterprise Information Security



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

senate.reception@senate.ucsb.edu
(805) 893-2885
<http://www.senate.ucsb.edu>

Joel Michaelsen, Chair
Claudia Chapman, Executive Director

January 11, 2007

John Oakley, Chair
Academic Council

RE: UCITTP Proposed Policy on Stewardship of Electronic Information

Dear John,

The Santa Barbara Senate has concluded its review of the proposed policy on stewardship of electronic information. Overall, we believe in and support the intent of the document, however, there are two broad concepts and also a couple of specific components that should be resolved.

The broader issues concern the proposed policy's notion of accountability, and the lack of attention to the long-term dimensions of stewardship. For instance:

1. The Draft's notion of accountability, as expressed in the initial paragraphs and in section 2, is overbroad. Whereas the foundation document "Statement of Ethical Values" reads:

"We will be accountable as individuals and as members of this community for our ethical conduct and for compliance with *applicable* [emphasis added] laws and University policies and directives"

the draft states:

"All members of the University community are accountable for compliance with University recommended guidelines, procedures, and practices for management of electronic information resources"

and:

"Each University department and individual is responsible for becoming familiar with and adhering to these guidelines."

However, the draft as constituted is clearly unsuitable for universal distribution. It is written in the language of IT professionals (e.g. "authenticated network proxy servers"), and it presumes familiarity with at least a dozen additional policies. If the intent is to articulate stewardship principles for which literally every member of the UC community can be held accountable, then this should be done in a separate, much briefer "executive summary" or some such.

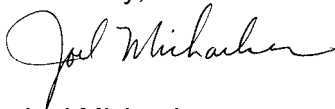
2. The term "stewardship" implies a *long-term* commitment to maintenance, yet the document focuses on short-term issues such as security and accessibility. There is no discussion at all of policies related to archiving, preservation, or long-term survivability of information. (The referenced "Records retention and disposition" policy focuses narrowly on administrative records, and makes only a coarse distinction between less than or more than 5 years.) The policy should either be retitled, to avoid conflicting with the commonly understood meaning of stewardship, or should be extended to address longer-term issues.

The more specific components requiring clarification generally concerned broad statements regarding limitations on software or equipment purchases that may prove problematic depending on how they are applied. Specific concerns were expressed regarding two components of the proposed policy:

1. Section 4. Part B, final paragraph. The statement that "Campuses should also identify and prohibit the use of specific software that is determined to pose security risks" should be clarified. Without additional details, one could envision a scenario where a software package used by a faculty member is considered a security risk and prohibited, adversely impacting faculty research. Identifying software that represents potential security risks is clearly important, but raises questions regarding what kinds of software this policy is targeting and how widely they might be in use.

2. Section 7, second to last paragraph. The statement that "campuses should ensure that purchases of technology-based high-value goods and services receive appropriate review," and that they conform with campus architecture and comply with licensing requirements, caused concern. We are in full agreement regarding licensing requirements, but the statement requiring "appropriate review" of high-value technology-based goods and services needs clarification. A major concern is that the University of California avoid adopting a highly-restrictive model that limits the types of purchases to specific vendors and models, thereby limiting the potential of researchers to push the technological envelope. While systems and software compatibility across campus is desirable, it would be detrimental if this effort led to a sacrifice of innovation and academic freedom.

Sincerely,



Joel Michaelsen
Divisional Chair

Cc: Executive Council