May 5, 2025

Kathleen Bawn
Chair, UCLA Academic Senate

Dear Kathy,

Thank you for the Senate's comments. We appreciate the time taken to review the draft policy.

There were two goals to the proposed revisions: (1) streamline the policy to focus on the obligation of workforce members to report if they become aware of the possibility of an information security incident; and (2) clarify the language used so that Policy 420 uses the same terms-and in the same way—as UC policies in this space.

We appreciate the concerns raised regarding (1) the definition of "Institutional Information;" (2) allowing for shifting costs to organizations; and (3) holding Unit Heads accountable for policy violations in their unit. As laid out below, however, those elements (some of which are not changes to the existing Policy 420) are dictated by UC policy.

1. **<u>The Definitions Come from UC Policies</u>**

   Policy 420 is but one of a number of policies issued by the University of California and its campuses related to information security. In particular, Policy 420's definition for "Institutional Information" comes from a long-standing UC definition. https://security.ucop.edu/files/documents/policies/it-policy-glossary.pdf

   Although we appreciate the sensitivity around ownership of intellectual property, this policy does not redefine those rights. The IT Policy Glossary includes defined terms "*relevant to using UC's IT and information security policies and standards*." (emphasis added). The definition of "Institutional Information," therefore, does not upset understandings around ownership (which are defined by other policies) when it defines which information that is compromised must be reported pursuant to UC and UCLA policy. The draft policy simply directs personnel to report incidents, and suspected incidents, affecting information.

   Second, as a matter of consistency, it is impractical to adopt a definition inconsistent with UC policy on information security. It would create mischief were UCLA to use a separate definition for "Institutional Information" that does not align with and would have differing obligations within a federated system.

   Finally, although the Senate proposed that the definition of Institutional Information consider the seriousness of any particular incident, such a sliding scale risks ambiguity. Among other things, the apparent scope of an incident could change over time. Accordingly, varying the definition would render consistent and timely reporting impossible, and would likely increase confusion about when matters need to be reported.

Far easier to report when there is an incident, or suspected incident, particularly when it does not upset long-standing understandings regarding intellectual property rights.

For those reasons, prudence favors keeping the UC definition of "Institutional Information" in the UCLA policy.

2. **Longstanding UC Policy Directs that Organizations May Be Accountable for Policy Deviations But the Revised Policy Introduces Needed Flexibility**

Many of the concerns expressed in the Senate's correspondence relate to the draft policy's framework that permits—but does not require—that costs related to incidents be assessed to organizations responsible for breaches in policy that lead to cyber incidents. Among other things, the Senate expressed concern that where individuals have multiple affiliations, it may be unfair to sanction an organization. Likewise, if the implication is a reduction in funds, the Senate contends accountability might undermine an organization's ability to conduct research or teaching.

As a threshold matter, however, the accountability provisions are not a change to Policy 420. The legacy Policy 420 contains an accountability element. In fact, the legacy policy *required* the assignment of costs.

> Any financial liability to, or costs incurred by the University resulting from a Suspected Security Breach or actual Security Breach in an Organization, or failure by an Organization to comply with this Policy, *shall* be assigned to that Organization.

(Emphasis added). The revised policy addresses the potential risks identified by the Senate to clarify that cost shifting, while permissive, is not required.

> Organizations *may* bear all or some of UCLA's direct costs that result from an Information Security Incident under the Organization's area of responsibility if the Information Security Incident resulted from a significant failure of the Organization to comply with this Policy.

(Emphasis added). Consequently, rather than mandate the shifting in costs, the revised policy would address the potential unfairness identified by the Senate (where responsible people might have multiple affiliations) by not requiring the assignment of costs but instead inviting a consideration of the full context to determine whether cost shifting is equitable.

The concern about limited resources, too, favors holding organizations accountable rather than not. While cost shifting to organizations deemed responsible for an incident might ultimately affect the research and teaching functions of such an organization, that is the havoc caused by large scale information security incidents, not the policy. The policy merely aligns incentives with productive behavior. If, through an organization's conduct,

there have been policy violations that result in cyber breaches, those organizations should be accountable and not pass those costs on to the rest of the enterprise, which also are responsible for research and teaching.

Significantly, however, the policy's assignment of accountability is dictated by UC Policy. IS-3 provides:

> Units may bear some or all of UC's direct costs that result from an Information Security Incident under the Unit's area of responsibility if the Information Security Incident resulted from a significant failure of the Unit to comply with this policy. These 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.

That systemwide mandate directs the accountability structure in Policy 420.

It also bears note that history also suggests that this policy does not create negative consequences described in the Senate's correspondence. Although UCLA has been the victim of breaches, the legacy policy did not create a situation where organizations were depleted through cost shifting. In the past (in the litigation context and elsewhere), cost shifting has resulted in repayment plans over years to balance accountability with operational needs.

Finally, the correspondence suggested the Policy sought to assign responsibility but did not provide the resources to address how to deal with breaches. The policy does, however, include a link to provide quick reporting, https://ociso.ucla.edu/report-cyber-security-concern. More to the point, however, the policy must be viewed in the context of the numerous training and communication resources available to community members to advise them on how to report incidents. https://ociso.ucla.edu/contact-us. UCLA also offers substantial training resources, https://ociso.ucla.edu/resources/training-courses, which includes the mandatory cyber training course required of all employees, as well as specialized resources for organization heads, https://ucla.app.box.com/s/wdl3x81d6lnl64a9m7bw2dmp2i7pf3de. As a consequence, while the policy does not, in its text, provide resources, substantial resources exist.

3. UC Policy Requires Accountability for Unit Heads

Finally, the Senate expressed concern that so-called Unit Heads may be held personally accountable for incidents, not in the form of several liability, but because advance approval from the Chancellor *may* be required before receiving merit increases if units are found to be non-compliant. In a related concern, the Senate expressed concern that

the policy may hold Deans responsible for not reporting prior to completion of a triage effort. Once again, although the drafters recognize that the assignment of individual accountability is new to Policy 420, the principle is once again required by UC Policy IS-3.

Systemwide information Security Policy IS-3 defines "Unit Head" as a senior leader responsible for information security within their unit. ("A generic term for dean, vice chancellor, vice provost or person in a similarly senior role who has the authority to allocate budget and is responsible for Unit performance... Unit Heads have important responsibilities to ensure effective management of cyber risk.") The policy goes on to describe substantial responsibilities entrusted to those leaders, including:

- Ultimate responsibility for execution of the policy within the Unit.
- Identification and inventory of Institutional Information and IT Resources managed by the Unit.
- Ensuring that Risk Assessments are complete and Risk Treatment Plans are implemented.
- Specification of the Protection Level and Availability requirements to Service Providers who manage IT Resources on behalf of the Unit.
- Through the risk management process, protection of Institutional Information and IT Resources managed by Service Providers through adherence to this policy. Through the risk management process, oversight over Institutional Information and IT Resources managed by Suppliers to ensure it meets the requirements of this policy.
- Ensures the above responsibilities are included in the overall Unit planning and budgeting process.

The systemwide policy also explicitly assigns responsibility for certain kinds of reporting to Unit Heads:

Reports Information Security Incidents to the CISO [as well as] any information security policy or standard that is not fully met by the Unit, or by a Service Provider managing Institutional Information or IT Resources on behalf of the Unit.

See also ("Workforce Managers and Unit Heads must promptly report Information Security Incidents involving Institutional Information classified at Protection Level 3 or higher to the CISO.") Unit heads also must report noncompliance with certain legal or contractual obligations ("Unit Heads must report to the CISO any non-compliance with legal and contractual requirements related to information security.")

In addition to directing responsibility, IS-3 assigns accountability to Unit Heads for fulfilling those responsibilities. ("The Unit Head is accountable for appropriately protecting Institutional Information and IT Resources, and for managing information

security risk in a manner consistent with this policy.") Pursuant to the UC President's February 26, 2024 letter on cyber investments, "Merit increases for unit heads whose units are found to be non-compliant require approval from the Chancellor."

The interplay between triage and notification does not justify a different result. IS-3 envisions reporting of "suspected" incidents without delay. After all, IS-3 and other policies therefore recognize that Unit Heads do not operate alone. IS-3 recognizes that in fulfilling these responsibilities, Unit Heads may appoint Unit Information Security Leads to assist in implementation and remediation.

Finally, and crucially, it is important to note that while the draft policy recognizes that leaders can be held accountable for non-compliance, Policy 420 does not compel a compensation implication. The policy merely implements what is directed by IS-3, namely, that leaders may be held accountable for the systems that they are indispensable parts of overseeing. At the same time, consequences must be judicially evaluated within administrative and HR structures.

4. **<u>The Policy Is Not Designed to Address Notice to Individual Victims</u>**

   Finally, the Senate suggests the policy should include information on how victims whose information was impacted by an incident are informed. The drafters respectfully disagree. This policy is designed to address how incidents are identified. It is not practical to address notice to potentially impacted individuals in this policy given the host of factual and legal implications that inform such notifications.

Sincerely,

Darnell Hunt
Executive Vice Chancellor and Provost

Lucy Avetisyan
Associate Vice Chancellor and Chief Information Officer

cc: April de Stefano, Executive Director, Academic Senate
Yolanda Gorman, Senior Advisor to the Chancellor and Chief of Staff
Andrea Kasko, Immediate Past Chair, Academic Senate
Mark Krause, Associate Vice Chancellor and Chief Compliance and Audit Officer
Emily Le, Principal Policy Analyst, Academic Senate
Megan McEvoy, Vice Chair/Chair Elect
Adriana Rosalez, Administrative Analyst, Academic Senate
Emily Rose, Assistant Provost & Chief of Staff to the EVCP