



# OFFICE OF THE CHANCELLOR

## UNIVERSITY OF CALIFORNIA, SANTA BARBARA

---

February 1, 2016

Dear Colleagues,

I write to share with you the attached letter from UC Executive Vice President and Chief Operating Officer Rachael Nava regarding UC cybersecurity.

Sincerely,

Henry T. Yang  
Chancellor

---

EXECUTIVE VICE PRESIDENT - CHIEF OPERATING OFFICER  
OFFICE OF THE PRESIDENT  
1111 Franklin Street, 12th Floor  
Oakland, California 94607-5200

February 1, 2016

UC FACULTY

Dear Colleagues:

I am writing to follow up on earlier discussions about cybersecurity matters across the UC system and to share to the fullest extent possible the principles and considerations that guide the University's efforts to respond to cyber attacks.

First, I want to thank you for sharing your concerns that we maintain the privacy protections enshrined in University policy even as we significantly strengthen our cybersecurity posture. As explained below, I do not believe these imperatives conflict; in fact, they reinforce one another in crucial ways. I would like to share some key principles and practices that help ensure that privacy protections are consistently upheld in the context of network security activities, some observations about the serious cyber attack we experienced at UCLA, and information about increasingly challenging attacks that are rising at academic institutions across the country.

As you know, on July 17, 2015, UCLA publicly announced that it had suffered a serious cyber attack. The attack appears consistent with the work of an Advanced Persistent Threat actor, or APT. An APT generally emanates from an organized, highly skilled group or groups of attackers that orchestrate sustained, well-planned attacks on high-value targets. Today, much effort in the cybersecurity industry is focused on APT attacks because they are difficult to detect and highly destructive. While there is no evidence that cyber attackers actually accessed or acquired any individual's personal or medical information at UCLA, the University decided to notify stakeholders. UCLA notified 4.5 million patients about the cyber attack. Within days, several lawsuits were filed against the Regents alleging various violations of State law, all 17 of which are now pending.

The UCLA attack, while exceptional in some respects, is part of an increasing trend of cyber attacks against research universities and health care systems. Institutions of higher education are increasingly targets of APT attacks because academic research networks hold valuable data and are generally more open. Indeed, the mission of our University is to promote knowledge sharing and research collaboration, which involves responsibly sharing data. A recent report from Verizon described educational institutions as experiencing "near-pervasive infections across the majority of underlying organizations," and observed that educational institutions have, on average, more than twice the number of malware attacks than the financial and retail sectors combined.

APTs seek to illicitly harvest credentials across academic networks and then use those credentials, and the trust relationships among systems, to move laterally to other nodes in a given network. There are techniques to address such attacks, but I share these points to underscore the seriousness of the threat posed by APT attackers and the fact that, for cybersecurity purposes, a risk to what appears to be an isolated system at only one location may in some circumstances create risk across locations or units.

In recognition of these realities, President Napolitano has initiated a series of system-wide actions to strengthen the University's ability to prevent, detect, and respond to such attacks. I believe these efforts are consistent with the reasonable expectations of the University community--our students, faculty, staff, patients, research sponsors, and academic partners--that we undertake serious efforts to protect sensitive data from malicious attacks. I also believe these actions are fundamental to realizing the University's commitment to privacy. The following actions were taken:

- A leading cybersecurity firm was engaged to assist the University in responding to the cyber attack, in part by analyzing network activity at all UC locations to detect and respond to any APT activity;
- Every location submitted a 120-day cybersecurity action plan to harden systems and improve administrative and physical safeguards;
- A Cyber-Risk Governance Committee (CRGC) was established, with representation from across the system, including the Academic Senate, to oversee

and guide system-wide strategies and plans related to cybersecurity. The CRGC has met several times already and is identifying key ways to strengthen our security posture while honoring the University's commitment to academic freedom, privacy, and responsible fiscal stewardship;

- A system-wide incident escalation protocol was developed to ensure that the appropriate governing authorities are informed in a timely way of major incidents; and
- Mandatory cybersecurity training was rolled out to all UC employees by October 1, 2015.

Several faculty members have requested detailed, technical information about the UCLA attack and the specific security measures taken in its immediate aftermath. I understand that some are concerned that such measures may have exceeded the University's policies governing privacy. I believe such actions were well within the operational authority of the University and in alignment with policy. It is regrettable that as long as the UCLA incident remains the subject of pending legal matters, I cannot publicly share additional information that might correct some of these misimpressions. As a policy matter, however, I wish to address the privacy and governance concerns that arise in the context of data security, without any express or implied reference to the UCLA attack.

With respect to privacy, the letter and structure of the University's Electronic Communications Policy (ECP) reflect the principle that privacy perishes in the absence of security. While the ECP establishes an expectation of privacy in an individual's electronic communications transmitted using University systems, it tempers this expectation with the recognition that privacy requires a reasonable level of security to protect sensitive data from unauthorized access. For this reason, the ECP expressly permits routine analysis of network activity "for the purpose of ensuring reliability and security of University electronic communications resources and services." (ECP, IV.C.2.b.) It expressly permits analysis of "network traffic" to "confirm malicious or unauthorized activity that may harm the campus network or devices connected to the network." (ECP, V.B.) Significantly, "consent is not required for these routine monitoring practices." (Emphasis added.) In short, the ECP reflects that, in some circumstances, the protection of privacy actually requires limited examination of electronic communications. (ECP, Attachment 1, V.A (noting that failure to prevent unauthorized access itself undermines privacy and confidentiality).) This is consistent with fair information practice principles and the University's duties under laws and regulations that require the use of physical, technical, and administrative safeguards to secure sensitive information.

The University takes great care to ensure that its practices reflect the balance outlined in the ECP. I would like to illustrate significant measures that we undertake to honor privacy rights in responding to a cybersecurity threat.

Even in time-sensitive circumstances, privacy impacts are typically evaluated before undertaking a coordinated network security effort. Appropriate privacy protection measures are embedded into the underlying scope of work both at the planning and execution stages of a network security effort. Such analysis typically includes an evaluation of the specific technical and analytic techniques to be used and whether they are consistent with the ECP. It also often means defining an appropriately limited scope for network analysis activity, focusing such analysis on known signatures for APT activity and related indicators of compromise. For vendors, the ECP requires scope discipline to be enforced by contract. (See ECP, IV.A (requiring vendors to be contractually bound to honor University policy).)

Layered review is another privacy-enhancing measure used in appropriate circumstances.<sup>1</sup> Layered review requires security alerts to be resolved in tiers, with each tier representing a limit on the type and amount of data to be reviewed. A layered review starts at the lowest tier, using automated review and basic metadata to resolve the security alert at that level. In circumstances where a security threat cannot be resolved at a lower tier or with automated means alone, the human-readable content of an underlying communication may be reviewed. The ECP limits such inspection to the “least perusal” necessary to resolve the concern. (ECP, IV.C.2.b & V.B.) To inspect content beyond what can be examined through “least perusal,” the ECP requires user consent or access without consent under a campus’s procedures, which typically involves a decision from the campus’s senior management.

I understand that some faculty members may be concerned about storage and use of data collected through network security analysis, including questions about data being used by the University for other, unrelated purposes. The ECP forbids the University from using such data for non-security purposes, (ECP, II.E.2, IV.A, & IV.C.2.b (prohibiting University employees from seeking out, using, or disclosing personal data observed in the course of performing university network security duties)), and violators are subject to discipline.<sup>2</sup> With respect to storage, much data collected through network analysis may already be stored elsewhere within the University’s network ecosystem (or even with third party cloud or other providers), independent of any network analysis activity. Data collected or aggregated specifically for network security purposes is only stored for a limited time, segregated in a highly secure system, and forensically obliterated thereafter. In some circumstances, a preservation of certain data related to litigation may be required by law, which may result in a longer storage period for a limited amount of network analysis data subject to such a mandate. With respect to third party requests for such data, the University has a long history of defending against improperly intrusive requests, including requests under the Public Records Act.<sup>3</sup>

Governance is also a critical aspect of this discussion. Ensuring that all stakeholders are fully enrolled in developing the University’s cybersecurity policies going forward is essential. As you know, the President has launched a coordinated system-wide initiative

to ensure that responsible UC authorities are appropriately informed about risks, that locations act in a consistent and coordinated way across the entire institution, and that the University can sustain action to manage cyber-risk. A number of structures have been put in place to elevate the importance of cybersecurity within University governance, some of which I described above but elaborate here for emphasis:

- The President asked the Chancellors to each appoint a single executive to lead efforts to review and improve cybersecurity at their location. These positions are the Cyber-Risk Responsible Executives (CREs), and each position reports directly to the Chancellor or location chief officer.
- A single escalation protocol has been implemented across the UC system to facilitate appropriate notification and handling of cybersecurity incidents. The protocol is intended to drive consistent analysis and response to cybersecurity incidents. It is being piloted and will be reviewed for effectiveness by the CRGC after six months.
- In addition to establishing the CRGC described above, the President has appointed a Cyber-Risk Advisory Board, composed of six internal and external expert advisors, to support the CRGC and provide information and advice about emerging issues and best practices in cybersecurity, and to help develop aggressive and effective approaches to managing cyber-risk, consistent with UC's teaching, research, and public service mission.
- Finally, a Cyber Coordination Center is being launched to help coordinate a variety of activities across the locations.

With specific reference to faculty governance, the President has reinforced with senior management the need for ongoing dialogue with our faculty and Senate leadership. The Senate has a robust presence at the CRGC, and I believe the CRGC is the best forum to develop mechanisms and policies for further ensuring that Senate leadership is fully engaged in policy development and briefed in a timely way regarding ongoing security matters and practices.

I also welcome a discussion about how to harmonize broader cybersecurity efforts with existing, campus-specific information governance guidelines. Some campus-level guidelines, established as part of system-wide information governance initiatives, limit the specific technologies and methods that may be used for network security activities, including some methods in ordinary use at other University locations and use of which may be necessary to comply with legal duties or to effectively evaluate a specific threat that may implicate multiple locations.

Given the difficult and shifting challenges worldwide in terms of cybersecurity, there is no monopoly on wisdom here. It is my intention to approach these issues with humility and openness, believing that our efforts will only be enriched by an exchange of ideas and viewpoints. I welcome your engagement on these issues and look forward to a deeper, joint effort to protect the privacy of our users and the security of the University's systems.

Sincerely,

Rachael Nava  
Executive Vice President - Chief Operating Officer

cc: Chancellors

---

<sup>1</sup> A layered review is not actually required by the ECP and may not be appropriate in all cases, but it illustrates the types of measures used to rigorously observe privacy principles.

<sup>2</sup> The ECP creates a specific exception for circumstances where an employee incidentally observes obvious illegal activity in the course of performing routine network security activities. (ECP, IV.C.2.b (defining exception for disclosure of incidentally viewed evidence of illegal conduct or improper governmental activity).)

<sup>3</sup> Public Records Act requesters may seek far more intrusive access to the content of faculty or staff records than what the ECP permits for network security monitoring. The limits on the University's own access to electronic communications under the ECP do not apply to Public Records Act requests.