AMERICAN ASSOCIATION OF UNIVERSITY PROFESSORS

555 New Jersey Ave., NW, Suite 600, Washington, DC 20001
PHONE: 202.737.5900 • **www.aaup.org**

October 23, 2025

Van Williams, Vice President of Information Technology Services and Chief Information Officer
University of California Office of the President
Via email to: van.williams@ucop.edu

Dear Mr. Williams,

The AAUP (American Association of University Professors) writes you with deep concern regarding the University of California Office of the President (UCOP) and UC campuses' continued implementation and expansion of the Trellix endpoint detection and response (EDR) surveillance software—despite the University of California systemwide academic senate resolution passed on June 12, 2025, calling for a halt to this program. We urge the University of California's Information Technology officers to honor this resolution and halt the use of Trellix EDR.

We appreciate that your office has pledged to follow AAUP guidelines in a letter dated May 27, 2025. Core to our guidelines are principles and practices of academic freedom and shared governance, both of which we find violated in UC EDR policies and practices.

Our guidance rests on two pillars, equally crucial.

First, the UC system's push to compel faculty to install Trellix EDR on their computers stands in opposition to the AAUP's long-established standards regarding academic freedom and electronic communications. Of particular relevance:

> Efforts to protect privacy in electronic communications are an important instrument for ensuring professional autonomy and breathing space for freedom in the classroom and for the freedom to inquire. (54)

Trellix's participation in the Joint Cyber Defense Collaborative, a federal initiative explicitly designed for rapid sharing of so-called threat information with government agencies, is a particular cause for alarm and suggests the distinct risk of warrantless governmental access to sensitive academic materials.

This risk is hardly hypothetical. The University of California system is being subjected to ongoing federal attacks, most recently resulting in UC Berkeley administrators capitulating to coercive federal probes for faculty names related to their free speech and their expertise. Trellix brings the risk of warrantless surveillance. It also brings the risk of surveillance by warrant, court order, or subpoena calling on the UC system to extract information from politically targeted faculty. This software undermines the

privacy of professors and anyone they interact with (students, staff, administrators, and the like) and their ability to engage in effective teaching and learning and freedom of assembly and speech, as well as threatens the security of their intellectual property. In addition, the top-down unilateral decision to adopt and enforce the use of this technology sets a poor precedent for shared governance of the university.

Second, AAUP shared governance standards regarding electronic communications provide that

> faculty members must participate, preferably through representative institutions of shared governance, in the formulation and implementation of policies governing electronic-communications technologies. (*Academic Freedom and Electronic Communications* 55)

And further that

> any new policy or major revision of an existing policy should be subject to approval by a broader faculty body such as a faculty senate. (55)

The UC Office of the President has not followed the UC systemwide academic senate assembly resolution. This resolution passed overwhelmingly, clearly recommending a statewide halt to the use of Trellix. On many campuses, UCOP implementations mandate that faculty install Trellix EDR software on all computers where university business is conducted, including teaching and research as well as those that manage private financial, medical, and other sensitive personally identifiable data. Once installed, Trellix EDR software grants unrestricted administrative or root-level access to faculty computers, enabling unchecked, comprehensive, and invasive monitoring, extraction, alteration, and even deletion of files without user consent or notification. This is an extraordinary intrusion into the privacy, right to freedom of expression, and intellectual security of faculty, which constitute core principles of the university's educational and research missions.

Some administrators have called Trellix "an industry standard," but we know that the chief information officer will appreciate and understand that the university's mission and its environment are fundamentally different from those of "industry." UC policy ignores the specific tasks of the professoriate for and its basis in academic freedom, jeopardized by generalized EDR software that grants centralized authorities root access to faculty machines.

The AAUP represents faculty across the University of California system who have participated in and are in agreement with the academic senate and the Council of UC Faculty Associations. We call for a halt to the installation of Trellix's invasive monitoring software, any other EDR software such as Crowdstrike or Sentinel One, or any other application with the ability to monitor the state, activities, or contents of faculty

machines, and for the adoption of less invasive cybersecurity measures. We also call on the UC system to affirm publicly its commitment to information technology that is protective of AAUP-supported principles of academic freedom and shared governance.

Sincerely,

Todd Wolfson, AAUP President
Mia McIver, AAUP Executive Director
Britt Paris, Chair, AAUP ad hoc Committee on AI in Academic Professions
Annie McClanahan, Council of UC Faculty Associations Copresident
Jessica Taft, Council of UC Faculty Associations Copresident