View in your browser

UC SANTA BARBARA

January 13, 2025

To: UCSB Campus Community

From: David Marshall, *Executive Vice Chancellor*
Josh Bright, *Associate Vice Chancellor for IT & CIO*

Campus Cybersecurity Updates

Cybersecurity is a campus priority in 2025 as UC Santa Barbara aims to comply with requirements mandated by the University of California Office of the President (UCOP). We are writing to provide an update on critical next steps and ask for your support, cooperation, and action.

Secure UCSB, our implementation plan to meet these requirements, has three key components—training compliance, network equipment upgrades, and device security implementation. In the weeks and months ahead, you will receive important communications about the following:

- **Cybersecurity Awareness Training:** all faculty, staff, and student workers are already required to complete annual Cybersecurity Awareness Training, along with other required trainings. **Anyone who has not completed the Cybersecurity Awareness training by March 31, 2025, will lose access to key web-based UCSB tools** (e.g. email, Zoom, Canvas). There will be multiple warnings and reminders before non-compliant users lose access. If users remain non-compliant, they will be redirected to the UC Learning Center to complete the required training before access is restored. (Please note that after July 15, 2025, the completion of all trainings mandated by law and UC policy will be required for access to campus network tools.)

- **Network outages:** please be aware that the installation of required new equipment in buildings throughout campus will cause planned, short-term service outages through May 2025. Plans for these temporary outages will be communicated directly to affected units at least two weeks in advance. Special considerations are being made for buildings where network downtime presents a safety risk or prevents a mission-critical activity. Employees may need alternate work accommodations while internet service is temporarily down. We ask for your patience and understanding as we complete these critical upgrades.

- **Device Security:** every UC-owned device is required to have campus-provided software that facilitates the deployment of cybersecurity tools. While ITS will provide support and guidance, the role of local IT personnel is critical in ensuring widespread implementation. Again, we ask for your cooperation and understanding as your local IT units make this crucial project a priority.

We understand that this may cause some to have concerns about privacy. **We want to be clear: installing the required cybersecurity tools on a UCSB-owned device does NOT provide access to your files, emails, browsing history, or any other standard, activity-related information.** The tools focus only on relevant data to determine if the devices are vulnerable to cyber threats. All tools must comply with the UC Statement of Privacy. You can read more about our commitment to respecting privacy here.

The success of the Secure UCSB initiative depends on all of us doing our part to ensure UCSB is compliant, especially completing your training and working with your local IT support staff to install the appropriate tools on your UC devices. The mandate outlines consequences should we fall short of compliance by the deadline, including requiring Chancellor’s approval for merit increases of unit heads whose areas are not in compliance.

If you have specific questions, they can be directed to secure-ucsb@it.ucsb.edu

Thank you for your continued commitment to advancing our institution’s cybersecurity. Cyberthreats are real–our campus blocks millions of such attacks every year–and all of us have a responsibility to protect sensitive personal and research data and ensure the viability and continuity of our research, educational, and public service missions.

Together, we can ensure UC Santa Barbara's secure and resilient future.