UCSF Health

May 6, 2025

Dear Colleagues,

Protecting UCSF Health from cybersecurity threats is a shared responsibility—and one that's increasingly important to the safety of our systems, data, and patients.

To support this, the University of California now requires all employees to complete cybersecurity training every year. This annual requirement reflects the reality that maintaining cybersecurity is an ongoing process—not a one-time task.

To meet this mandate, UCSF will begin disabling system access for anyone whose training is expired starting May 21, 2025. While we hope to avoid this, it's important to be aware that access to critical systems will be blocked if training is not completed on time.

What you need to do:

- Watch for reminder emails and complete your annual training before it expires.
- Check your status or take the training in the UC Learning Center. BCH Oakland employees can access the training here.
- Learn more on the Mandatory Training website.

What happens if your training expires:

- **After the deadline**: Your MyAccess account will be disabled, blocking access to systems like BearBuy, HBS/MyTime, DocuSign, and MyExpense.
- **30 days overdue**: You'll need to reset your Active Directory password daily.
- **60 days overdue**: Your Active Directory account will be fully disabled. A process is in place to support emergency access needs for patient care.
- **How to regain access**: Complete your assigned cybersecurity training. Access will be restored the following morning.

We recognize that many of you have limited time and access to a computer during your workday. We're committed to working with departments across UCSF Health to ensure you have the time, flexibility, and support needed to meet this requirement without adding undue burden.

Thank you for your continued attention to safety, security, and the standards that help UCSF Health fulfill its mission.

Sincerely,

Sheila Antrum
Senior Vice President and Chief Operating Officer
UCSF Health