

## Cybersecurity Training Enforcement Program

In February 2024, the [UC Office of the President issued a letter](#) requiring 100% of UC campus employees to be compliant with Cybersecurity Awareness Fundamentals training. For UC Davis to meet this mandate, we will begin enforcing completion of the UC Cybersecurity Awareness Fundamentals required training on July 1, 2026. The program's goal is completion before enforcement to avoid disrupting academic work.

**UC Davis graduate student employees and postdoctoral scholars who do not complete the UC Cybersecurity Awareness Fundamentals training by their individual deadline will temporarily lose access to core campus digital services until the training is completed.**

Digital services that will be temporarily restricted include:

- UC Davis Google Workspace
- UC Davis Box
- MyInfoVault (MIV)
- Aggie Enterprise
- Myucdavis

You can read more about digital service restrictions on the [Academic Affairs website](#).

If your access is restricted due to noncompletion of the UC Cybersecurity Awareness Fundamentals training, access will be restored within a few hours of verification that you have completed the training.

### What do I need to do?

Check your training status and due date by logging in to the [UC Learning Center](#) and selecting the **Required Training** section. Deadlines to complete the UC Cybersecurity Awareness Fundamentals training are based on when you last completed the module. Be sure to complete the training and remain up to date on all mandatory training programs.

### How will I know when my training is due?

The [UC Learning Center](#) notifies employees that training is due with email reminders beginning 30 days before the deadline, with subsequent email reminders two weeks, one week, two days, and one day prior to expiration. Employees will also receive login screen messages beginning two weeks prior to the deadline.

## Who does this apply to?

The UC Cybersecurity Awareness Fundamentals training is required of **all UC employees** on active pay status including, but not limited to, faculty, all academic titles, visiting faculty, recall faculty, international scholars, Continuing and Professional Education instructors, staff, undergraduate and graduate student employees, and postdoctoral scholars.

While this compliance effort currently applies only to the UC Cyber Security Awareness Fundamentals training for employees on the Davis campus, it will eventually expand to include additional required training courses and other employee populations in future phases.

## Can I request a deadline extension?

Individuals with special circumstances may request a one-time seven-day extension through their department's academic personnel contact. Graduate student employees with questions can also contact their graduate program/group coordinator.

## Where can I get more information or help?

For more details and updates, see the [Training Compliance Program on the Academic Affairs website](#). Graduate student employees should contact the HR person in their department or reach out to their graduate program/group coordinator for support. Postdoctoral scholars should reach out to their academic point of contact.

## Cybersecurity is a shared responsibility

Maintaining the security of our systems is critical to fulfilling our research, teaching, and service mission, and every one of us shares that responsibility. That is why UC Davis is joining several of our sibling campuses, including UC San Diego and UC Irvine, in taking this step to protect shared university systems, research data, and our broader UC mission.

Thank you for doing all you can to keep our information secure at UC Davis.

Sincerely,

Jean-Pierre Delplanque  
Vice Provost & Dean,  
Graduate Studies

Aisha Jackson  
Chief Information and Digital Strategy Executive

