UCOP Cybersecurity Mandate 2025

UCR's plan to better protect our campus &
respond to new UC system-wide requirements

Dewight Kramer
Chief Information Security Officer

UC RIVERSIDE
Information Technology Solutions

UNIVERSITY OF CALIFORNIA

Michael V. Drake, MD
President

Office of the President
1111 Franklin St.
Oakland, CA 94607

universityofcalifornia.edu

CAMPUSES
Berkeley
Davis
Irvine
UCLA
Merced
Riverside
San Diego
San Francisco
Santa Barbara
Santa Cruz

MEDICAL CENTERS
Davis
Irvine
UCLA
San Diego
San Francisco

NATIONAL LABORATORIES
Lawrence Berkeley
Lawrence Livermore
Los Alamos

DIVISION OF AGRICULTURE AND NATURAL RESOURCES

February 26, 2024

CHANCELLORS

Dear Colleagues:

As you know, protecting the University's sensitive information and systems is of paramount importance. To strengthen our cybersecurity posture and mitigate potential risks, we are requesting submission of an updated information security investment plan.

Plan Expectations:

Your plan should outline your location's strategy for achieving the following key outcomes by May 28, 2025:

- Standards compliance:
  - Ensure cyber security awareness training for 100 percent of location employees.
  - Ensure timely cyber escalation of incidents in alignment with UC Incident response and cybersecurity escalation standards.
- Controls compliance:
  - Ensure identification, tracking and vulnerability management of all computing devices connected to university networks.
  - Deploy and manage UC-approved Endpoint Detection and Recovery (EDR) software on 100 percent of assets defined by UC EDR deployment standards.
  - Deploy, enable, and configure multi-factor authentication (MFA) on 100 percent of campus and health email systems in conformance with established UC MFA configuration standards.
  - Deploy and configure a robust DLP solution for all health email systems to mitigate unauthorized data exfiltration.

Scope:

The investment plan should include:

- All location units including but not limited to AMCs, schools, divisions, departments, and centers regardless of whether their IT infrastructure is managed centrally.
- All employees (inclusive of faculty).

Timeline and Reporting:

- Plan Submission: Please submit your updated comprehensive information security investment plan to interim CISO, Monte Ratzlaff (Monte.Ratzlaff@ucop.edu) by April 30, 2024.
- Plan Completion: Plan outcomes should be achieved by May 28, 2025.
- Progress Reports: Please submit written progress reports to interim CISO Monte Ratzlaff on June 30, 2024; August 30, 2024; October 30,2024; January 30, 2025; and March 28, 2025. Progress reports should be discussed as part of your location's bi-annual digital risk meetings.

Supporting Resources:

To support the execution of the investment plan, the Office of the President makes the following resources are available:

- Cyber Risk Coordination Center
- Be Smart About Cyber and Safety Programs
- ECAS Audit Advisory Services
- UC Threat Intelligence Services
- UC Threat Detection and Protection Services
- UC Security Risk Assessments
- UC Cybersecurity Consulting Services

Non-Compliance Consequences:

We understand that achieving these goals requires dedicated effort and resource allocation. However, failure to comply with these requirements will have significant consequences, including:

- Non-compliance with any outcomes stated above will result in a 15 percent increase of your location's cyber insurance premium, reflecting the elevated risk posed to your location and the system.
- Non-compliant units will be assessed all or part of the costs related to security incidents up to $500,000 that are a result of the failure to comply with these requirements.
- Merit increases for unit heads whose units are found to be non-compliant require approval from the Chancellor.

We are confident that all locations share our commitment to protecting our vital information and systems. We encourage you and your teams to utilize the resources available through UC IT and the Cyber-risk Coordination Center to develop and implement your plans effectively.

We appreciate your cooperation and look forward to receiving your information security investment plans by the deadline.

Sincerely,

Michael V. Drake, MD
President

UC President's Letter: Outcomes to Be Achieved by May 2025

100% Compliance with UC cybersecurity awareness training

UCR is at ~86%

100% Compliance with multi-factor authentication on all email systems

UCR is at ~90%

100% Inventory and management of devices and vulnerabilities [1]

UCR is at ~30%

Data Loss Prevention tool configured on health email system

UCR and UCR Health is at 0%

100% Compliance with Endpoint Detection and Response software

UCR is at ~60%

Timely escalation of incidents and a documented program

UCR is at ~100%

1: Devices are laptop, desktop, and servers. Students are exempt. There are other special cases that will also be exempt or allowed to seek an exception.

Why This Mandate?

1. To better protect our people and our mission

2. To defend against the exponential increase in cyber threats that target higher education

   As a result, UCOP has advised of campus consequences for non-compliance

June 20, 2024

RANSOMWARE ATTACK FORCES PERMANENT CLOSURE OF 157-YEAR-OLD COLLEGE

Hackers breached the college's systems and gained access to institutional data, halting school operations.

READ MORE »

June 19, 2024

UNIVERSITY OPERATIONS SHUT DOWN AND CLASSES CANCELED AFTER RANSOMWARE ATTACK

Hackers breached the university's systems, encrypting critical data and disrupting campus activities.

READ MORE »

May 14, 2024

CYBERCRIMINALS EXPOSE UNIVERSITIES' SENSITIVE DATA

A ransomware group exploited a vulnerability found in a software product used for file transfers, breaching sensitive data repositories and compromising confidential information.

READ MORE »

April 24, 2024

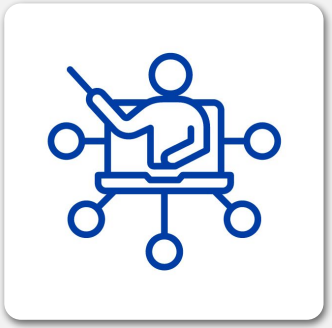
UNIVERSITY LOSES $1.9 MILLION AFTER FALLING VICTIM TO BUSINESS EMAIL COMPROMISE

Hackers successfully tricked university employees into transferring a substantial amount of money to a fraudulent bank account under the guise of a legitimate contractor.

READ MORE »

What's My Role?

The tools will be provided to employees at no cost. Employees who use devices that are not managed by ITS or their local IT department will need to install the tools themselves.



Complete UC Cyber Security Awareness Fundamentals training

Install and use the three UCR-supplied security tool applications

Use the DUO mobile app to authenticate into UCR systems

These are vital and urgent first steps we must take to enhance UCR's security posture and align with UC cybersecurity expectations. The campus can expect that additional measures may be implemented as UCR works to come into full compliance.

What's My Role?

In an effort to mitigate the campus consequences outlined in the President's letter, UCR must address non-compliance via:

- Restricted access to campus resources such as networks, WiFi, and online service applications
- Other potential repercussions currently being determined by campus leadership

These measures are necessary to help ensure the safety and security of both the UCR community and our larger UC community.

Timeline to Meet May 2025 Deadline

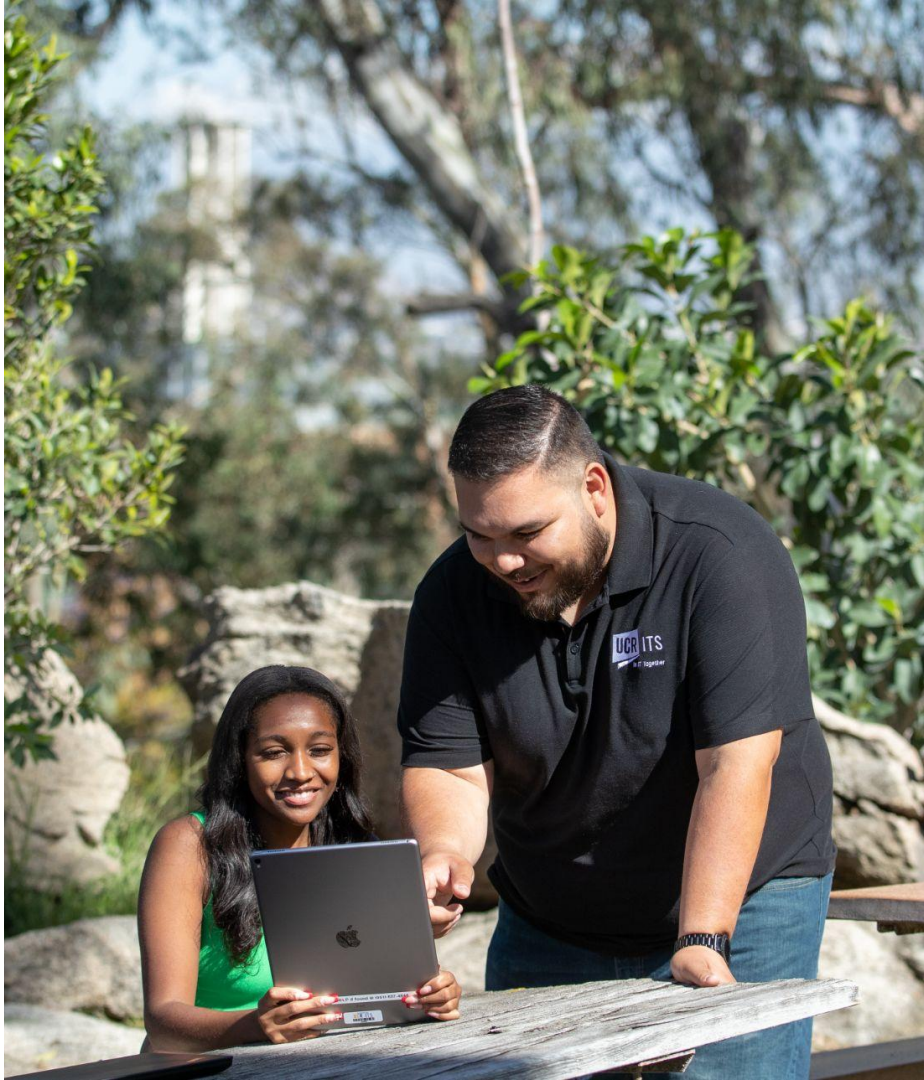
Available Support

Now

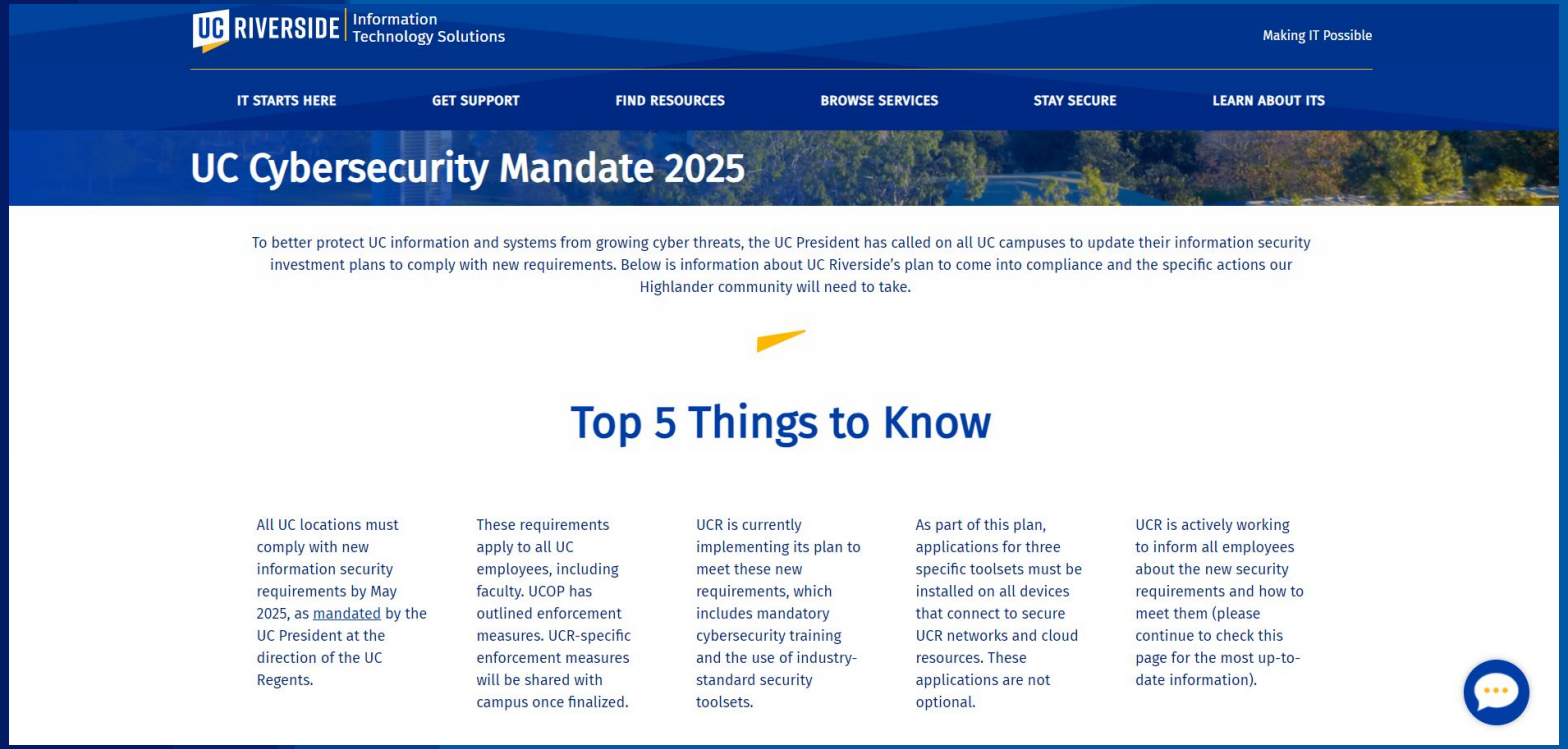
- Initiative website with info, resources, FAQs
- UC Learning center to access training
- Department meetings & campus presentations

Coming Soon

- Toolset downloader
- Self-help articles in the Knowledge Base
- Pop-up help desks & office hours



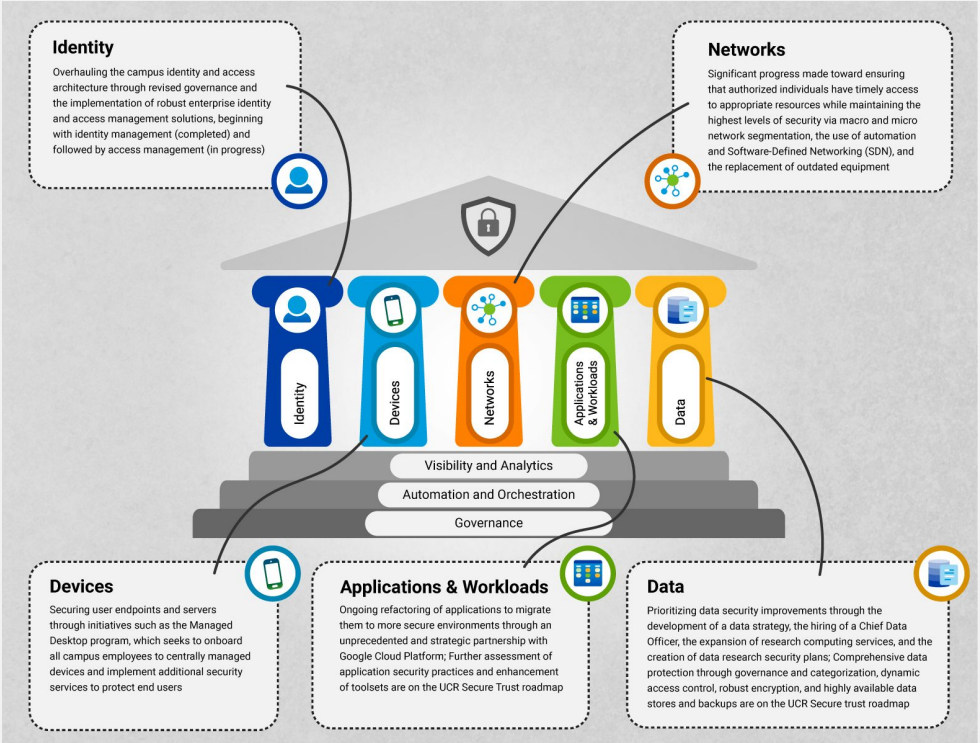
Stay Informed: its.ucr.edu/cybersecurity-mandate-2025



Security Investment Roadmap

While the UC Cybersecurity Mandate 2025 catalyzes immediate action, it's important to understand that UCR has already embarked on a journey to enhance its information security through the **UCR Secure Trust program**.

- Built on five key pillars
- Mandate aligns with and reinforces the goals of UCR Secure Trust
- UCR Secure Trust provides a broader framework for continuous improvement and long-term cybersecurity resilience



Thank you!

UC RIVERSIDE
Information Technology Solutions