

Compliance Update

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

**100% Compliance with
UC cybersecurity awareness training**

UCR is at ~92%

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

UCR is at ~100%

**100% Inventory and management
of devices and vulnerabilities ¹**

UCR is at ~47%

**Data Loss Prevention tool
configured on health email system**

UCR and UCR Health is at 0% (testing)

**100% Compliance with Endpoint
Detection and Response software**

UCR is at ~67%

**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.

UCR's Compliance Plan

Training



April 13: Employees overdue on training will receive training prompt upon every UCR login.

June: Employees still overdue on training will be unable to access UCR resources until training is completed

Identity



Employees are strongly encouraged to enroll in more than one MFA method.

May 23: Sunsetting of support for HOTP devices will begin so employees will need to exchange for TOTP device, if needed

Toolset



May 23: UCR Leadership deadline for admin staff to move to Secured Device Service

May 28: UCOP & UC Regents to assess UCR's level of compliance

June: Devices that do not have the toolset installed will be prohibited from connecting to the secure UCR network

There are numerous steps UCR has taken behind the scenes to become compliant. However, there are three keys steps employees must take:

1. Take the UC training
2. Verify your identity
3. Download the security toolset

Toolset enforcement will be rolled out in phases, beginning with restricting access to certain UCR applications

Action Required

Any device that connects to secure UCR resources must have the UCR Security Toolset installed.

Scenario One: An employee who uses a personal device to conduct university business.

Example: A faculty member uses their own personal device to perform university work, including submitting grades and accessing research data.

Action Required: The employee must install the UCR Security Toolset on their personal device and any other non-managed (not managed by UCR IT) devices they use to connect to secure campus resources.

Note: If the employee does not wish to download the toolset on their personal device, they must use a university-issued device to perform university work.



Action Required

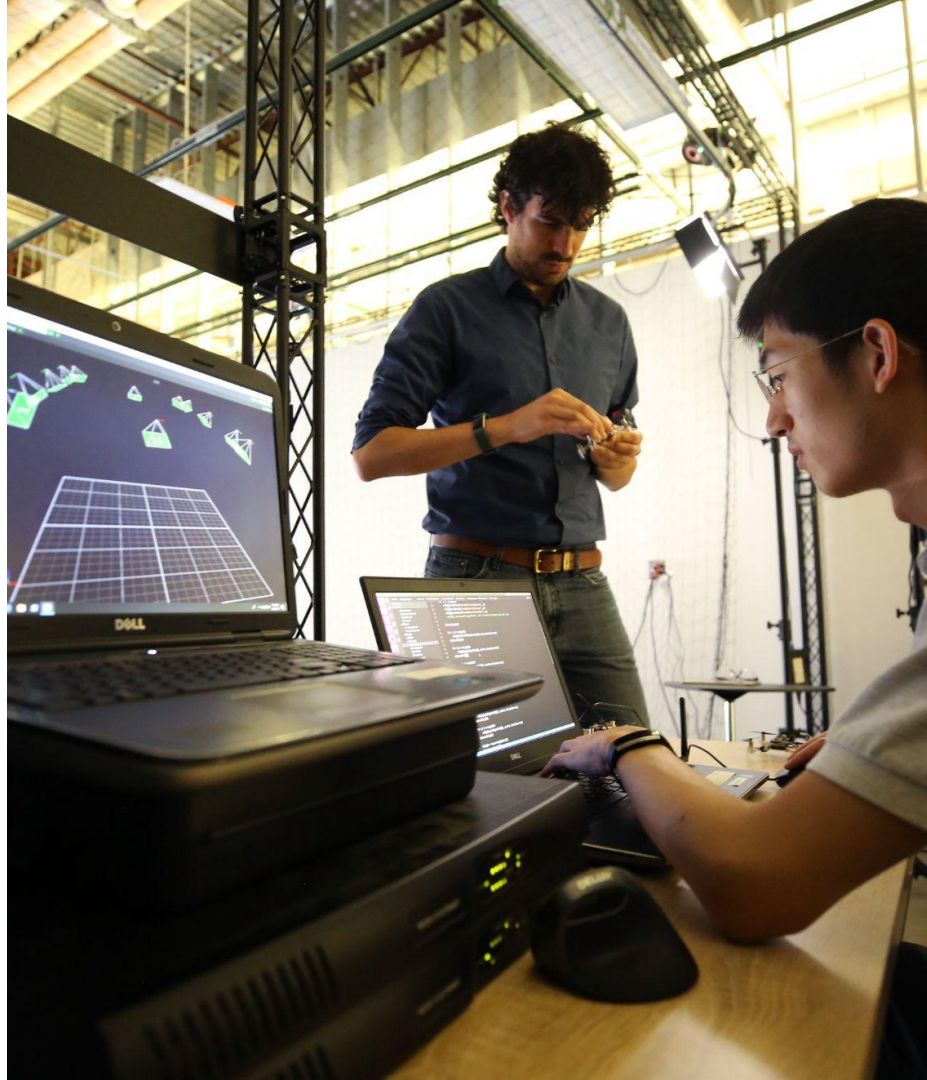
Any device that connects to secure UCR resources must have the UCR Security Toolset installed.

Scenario Two: A faculty member who uses a university-issued device that does not currently have the UCR Security Toolset installed.

Example: A faculty member who uses a device that was purchased with grant money that is not managed by IT.

Action Required: The employee must install the UCR-provided security toolset manually.

Note: Faculty can request for their university-issued device to become part of SDS.



Action Required

Any device that connects to secure UCR resources must have the UCR Security Toolset installed.

Scenario Two: An employee who uses a university-issued device that does not currently have the UCR Security Toolset installed.

Example: A staff member whose unit has not yet moved to Secured Device Services (SDS).

Action Required: The employee must attend an on-site opportunity to reimage their device and/or receive the needed updates.

Note: ITS is looking to coordinate with CFAOs and unit heads to move all units to SDS by May 23, 2025. In the unlikely event this date is not met, the toolset will need to be manually installed on all remaining devices.



Action Required

All UCR employees must be current on their required annual UC cybersecurity training.

Scenario Three: An employee is overdue on completing their UC Cyber Security Awareness Fundamentals training in the UC Learning Center.

Action Required: The employee will receive a reminder message every time they attempt to log into secure UCR resources. The employee must complete the training in order to be compliant.





Note: As with other HR requirements, ITS is looking to CFAOs and HR staff to enforce employee (including student employee) compliance with this training requirement. Unit compliance reports are being delivered to campus leadership.



Consequences of Noncompliance

- 1 **15% increase** in cyber insurance premiums
- 2 Up to **\$500,000** in costs for security incidents
- 3 Merit increases for unit heads will require Chancellor's approval

These risks should be considered in the context of current financial and legislative uncertainty in higher education

 <p>June 20, 2024</p> <p>RANSOMWARE ATTACK FORCES PERMANENT CLOSURE OF 157-YEAR-OLD COLLEGE</p> <p>Hackers breached the college's systems and gained access to institutional data, halting school operations.</p> <p>READ MORE »</p>	 <p>June 19, 2024</p> <p>UNIVERSITY OPERATIONS SHUT DOWN AND CLASSES CANCELED AFTER RANSOMWARE ATTACK</p> <p>Hackers breached the university's systems, encrypting critical data and disrupting campus activities.</p> <p>READ MORE »</p>	 <p>May 14, 2024</p> <p>CYBERCRIMINALS EXPOSE UNIVERSITIES' SENSITIVE DATA</p> <p>A ransomware group exploited a vulnerability found in a software product used for file transfers, breaching sensitive data repositories and compromising confidential information.</p> <p>READ MORE »</p>	 <p>April 24, 2024</p> <p>UNIVERSITY LOSES \$1.9 MILLION AFTER FALLING VICTIM TO BUSINESS EMAIL COMPROMISE</p> <p>Hackers successfully tricked university employees into transferring a substantial amount of money to a fraudulent bank account under the guise of a legitimate contractor.</p> <p>READ MORE »</p>
---	---	---	---

Available Support

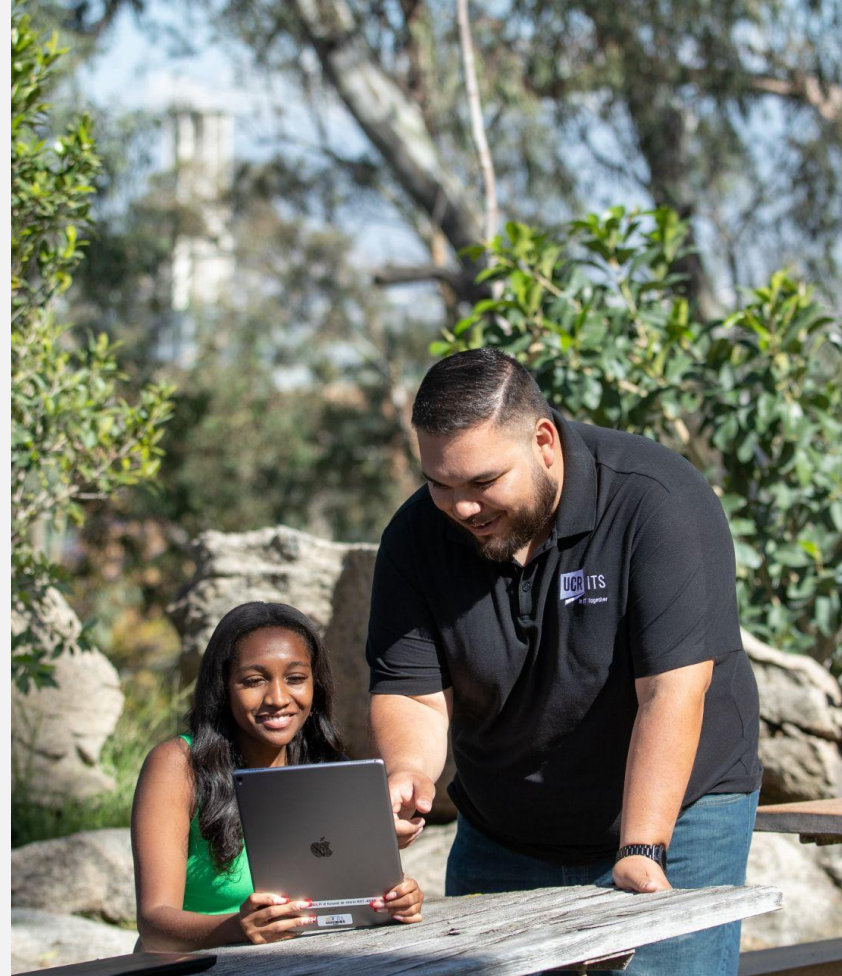
Support

- **In-person support** available 8:30 AM - 4:30 PM Monday - Friday at the IT Support stations in the Tomás Rivera Library, Orbach Science Library, and Student Success Center
- **Virtual office hours** with ITS (see events.ucr.edu for dates)
- **Secured Device Services** (SDS) will be **reaching out directly** to update computers and move units to SDS
- **Submit an IT ticket** at its.ucr.edu/help

Resources

- Learn about the toolset: its.ucr.edu/uc-security-toolset
- Download the toolset: endpointinventory.ucr.edu
- Take the required annual training: ucrllearning.ucr.edu
- Learn about MFA: its.ucr.edu/mfa
- Mandate homepage: its.ucr.edu/cybersecurity-mandate-2025

Request an exception for extraordinary circumstances (e.g., certain scientific equipment, HPCC, research databases with extreme sensitivities): [Information Security Consultation form](#)



Q&A: Which UCR Applications Will Be Used to Block?

Applications under consideration:

PIWRS, Kuali, LMS, Efile, Canvas, Rspace/Web

Applications not under consideration (initially):

Timesheets, Oracle Finance

Common Question: Can't we block using our Single Sign On page and just block everything?

Answer: Currently this is not possible but that is the goal long term.

Common Question: Can't we just block all of the UCR network?

Answer: Many of the UCR apps are not on UCR's physical network. Moreover, we need to make more progress with the network refresh before we can block the wired network.

Thank you!



Background



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 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

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 are the required services?



Inventory and Management
security tool applications



Vulnerability Scanning
security tool applications



Endpoint Detection and Response
security tool applications

*The tools are provided to employees at no cost at:
<https://endpointinventory.ucr.edu>*

Employees who use devices that are not managed by ITS or their local IT department will need to install the tools themselves.

What's My Role?



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 (e.g., Canvas, R'Space)
- 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

April 2024

**Awareness &
Engagement**

October 2024

**Protocol/Toolset
Training & Implementation**

January 2025

**Hypercare,
Reporting &
Assessment**

May 2025

**Enforcement &
Continuous
Improvement**

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

 **UC RIVERSIDE** Information Technology Solutions

Making IT Possible

[IT STARTS HERE](#) [GET SUPPORT](#) [FIND RESOURCES](#) [BROWSE SERVICES](#) [STAY SECURE](#) [LEARN ABOUT ITS](#)

UC Cybersecurity Mandate 2025

To better protect UC information and systems from growing cyber threats, the UC President has called on all UC campuses to update their information security investment plans to comply with new requirements. Below is information about UC Riverside's plan to come into compliance and the specific actions our Highlander community will need to take.

Top 5 Things to Know

All UC locations must comply with new information security requirements by May 2025, as mandated by the UC President at the direction of the UC Regents.

These requirements apply to all UC employees, including faculty. UCOP has outlined enforcement measures. UCR-specific enforcement measures will be shared with campus once finalized.

UCR is currently implementing its plan to meet these new requirements, which includes mandatory cybersecurity training and the use of industry-standard security toolsets.

As part of this plan, applications for three specific toolsets must be installed on all devices that connect to secure UCR networks and cloud resources. These applications are not optional.

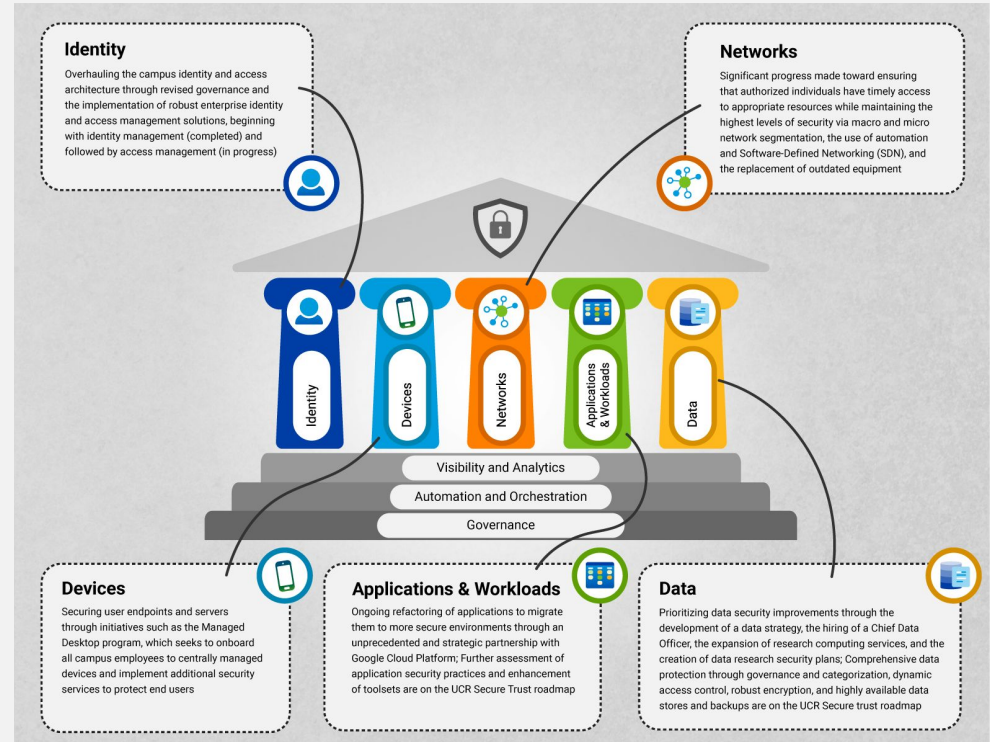
UCR is actively working to inform all employees about the new security requirements and how to meet them (please continue to check this page for the most up-to-date information).



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!

