UC RIVERSIDE
Information Technology Solutions

UCOP Cybersecurity Mandate 2025

The digital landscape is evolving, and with it, threats to our university's sensitive information and vital operations. The recent system-wide cybersecurity mandate requested by the UC Regents and led by the UC Office of the President underscores the critical need for proactive measures. UCR's response is not just about compliance with the UC Cybersecurity Mandate by May 2025, it's about fortifying our institution and safeguarding its future.

The Stakes Are High: Real-World Consequences

Recent incidents at universities across the nation underscore the devastating impact of cyberattacks:

- Data Breaches: Cybercriminals are increasingly targeting universities, exposing sensitive data. UC is not exempt, with UCLA having experienced a similar breach in May 2024.
- Financial Loss: Universities have suffered significant financial losses, with Southern Oregon University losing $19 million due to a cyberattack.
- Operational Disruption: Ransomware has crippled universities, such as Howard University, forcing cancellations of classes and research and harming institutional reputation.
- Institutional Closure: The dire consequences of a cyberattack can even lead to permanent closure regardless of legacy, as exemplified by 157-year-old Lincoln College.

UCR Leaders: The Key to Success

Change adoption research consistently demonstrates that leadership buy-in and active support are crucial for successful organizational change. Your commitment and engagement as a leader in your respective area is our best chance at achieving a secure UCR.

Campus Compliance: Your Role

In order for UCR to come into compliance with UCOP Cybersecurity Mandate 2025 by May 28, 2025, your support is essential to:

- **Foster understanding**: Clearly communicate the reasons behind the changes and the potential impact on your unit's operations. Information about this effort can be found on the mandate webpage.
- **Encourage participation**: Ask your team to 1) stay current on the UC cybersecurity training, 2) be advised of upcoming enhancements to multi-factor authentication (MFA), and 3) install and use the UCR security toolset on any device not managed by UCR ITS or a distributed campus IT partner.
- **Address concerns**: Openly discuss any challenges or apprehensions your team may have, and work collaboratively with ITS to find solutions.
- **Monitor and enforce compliance**: Ensure that the faculty and staff in your unit adhere to the requirements, including any additional measures that are identified as UCR works to come into full compliance.

Together, We Can Protect UCR

By working together, we can create a secure environment that fosters innovation and protects our university's mission. We urge you to embrace this change and actively lead your teams toward a culture of cybersecurity awareness and responsibility. Thank you for your leadership and partnership in securing UCR's future!

Learn more: its.ucr.edu/cybersecurity-mandate-2025