UNIVERSITY OF CALIFORNIA

Michael V. Drake, MD
President

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

universityofcalifornia.edu

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

cc: Executive Vice President and Chief Operating Officer Nava
Chief of Staff Kao
Vice President Williams
Chief Risk Officer Confetti
Interim CISO Ratzlaff
Chief Policy Advisor McAuliffe
Managing Counsel Sze