



COMPLIANCE ALERT

Brought to you by: Ethics, Compliance and Audit Services



[Audit](#) [Compliance](#) [Investigations](#) [Presidential Policies](#) [Contact](#)

This Issue's Contents

Audit and Investigations	1
Cybersecurity	1
General Compliance	2
Health Sciences Compliance	2
Human Resources Compliance	3
Research Compliance	3
Policy	4
Privacy	4

Audit and Investigations

[UC Office of the President Creates Audit Implementation Website](#)

To provide greater transparency towards the progress the University of California is making in implementing the California State Auditor's recommendations, the Office of the President has created the [UCOP Audit Implementation Plan website](#). The site will track the progress made on all 33 recommendations and includes periodic updates provided by the task force convened by UC President Napolitano. Some areas of focus include:

- Enhancing the UCOP budget process and presentation.
- Providing additional information on systemwide initiatives.
- Implementing a workforce and staffing plan.
- Reviewing expense policies and establishing a reserve policy.

Cybersecurity

[Ransomware Update](#)

There has been a lot in the news about ransomware lately. Recent ransomware attacks have caused high-profile business shut downs, including the San Francisco transit system fare gates, Hollywood Presbyterian, and the University of Calgary, just to name a few.

Ransomware is the fastest growing malware threat, targeting users of all types—from the home user to the corporate network. This article provides some background on what Ransomware is and how to protect yourself.

Here's What's Happening at ECAS

- ◆ New Senior Vice President and Chief Compliance and Audit Officer (SVP-CCAO)

The UC Regents appointed Alexander A. Bustamante as Senior Vice President and Chief Compliance and Audit Officer at UC Office of the President. The announcement was made during the Regents meeting held July 12-13 at UCSF. The new SVP-CCAO previously led as Inspector General of the Los Angeles Police Department (LAPD), implementing their compliance program and providing oversight since 2011. Prior to his service for the LAPD, the SVP-CCAO served as an assistant U.S. Attorney and as a Judge Advocate General for the U.S. Army. He is also a returning UC Berkeley alumni and is expected to commence his new role on September 5. Further information is available through the [UC press release announcement](#).

- ◆ ECAS is currently in the process of recruiting for the position of Systemwide Director of Investigations. Information for interested candidates was made available through the [UCOP Online Job Posting](#).
- ◆ Ethics and Compliance Training
 - ◇ General Ethics and Compliance Briefing online course update is estimated to roll out in September in order to enhance web accessibility.
- ◆ ECAS leadership presented to the Regents their 2017-18 Ethics and Compliance Program Plan, identifying key risk priorities. The plan is available through the [Compliance and Audit Committee online agenda](#).



COMPLIANCE ALERT

Brought to you by: Ethics, Compliance and Audit Services



[Audit](#) [Compliance](#) [Investigations](#) [Presidential Policies](#) [Contact](#)

What is ransomware?

Ransomware is a type of malicious software (a.k.a malware) that locks the victim out of their computer or files – often by encrypting them – until a ransom is paid. The ransomware typically displays a message letting the victim know that they have been locked out, along with instructions for how much and how to pay.

Ransomware is often spread through use of stolen credentials, malicious links and harmful attachments in email; however, this is not the only mechanism. Other sources include malicious applications and files, and adware/spyware.

It is important to note that paying the ransom doesn't necessarily guarantee that you'll get access to your computer or files back. In fact, a couple of recent, high-profile cyber-attacks, dubbed "WannaCry" and "Petya", even posed as ransomware to distract people from the real attack, but in those cases there was no way for people to get their files back by paying the ransom. The FBI and law enforcement advise never paying the ransom.

How to protect yourself

The following good cybersecurity habits will help to protect you from ransomware, and many other cyber threats as well:

- Back up critical files, and store the backups in a physically separate location from the originals.
- Always think twice before clicking on links or opening attachments.
- Keep a clean machine! Keep your devices, apps and browsers patched and up to date.
- Protect your passwords, and use multi-factor authentication wherever possible.
- If it's suspicious, report it!

What should you do if you get ransomware?

Most importantly, don't panic. If you have good backups, you're probably OK with some technical assistance. As mentioned above, report the incident so you can get help.

Additional information about ransomware:

<http://cio.ucop.edu/ransomware-rising-putting-our-files-at-risk/>

Eight Highly Effective Habits for Cybersecurity:

<https://security.ucop.edu/resources/security-awareness/habits.html>

FBI Guidance for Traveling Abroad

In order to combat potential cybercrime faced by professionals and students who travel abroad, the Federal Bureau of Investigation has developed brochures to guide how travelers can better secure their electronic devices.

- [Safety and Security for the Business Professional Traveling Abroad](#)
- [Safety and Security for U.S. Students Traveling Abroad](#)

General Compliance

Corporate Ethics Can't Be Reduced to Compliance

As organizations continue to grow in complexity, there is an alternative direction in which companies can take to curtail unethical behavior. It is suggested that simply increasing the number of rules offers a singular focus to compliance. Instead, organizations should focus their compliance efforts on the positive virtues they want workers to exhibit in order to reduce risk, maintain an innovative environment and foster communication.

The Emergence of Compliance: A new profession?

As the field of compliance has grown since its emergence, the number of issues it handles has increased to meet the different demands felt by institutions. Some have argued compliance should structurally be part of an organization's legal team. However, compliance officers and professionals continue to define compliance as a unique field capable of providing a cohesiveness amongst various parties and requiring skillsets beyond those provided through legal training.

Health Sciences Compliance

Careless Handling of HIV Information Jeopardizes Patient's Privacy, Costs Entity \$387K

The St. Luke's-Roosevelt Hospital Inc. has settled a potential HIPAA Privacy Rule violation with the Department of Health and Human Services by paying \$387,200. The potential violation consisted of a patient's medical information, including their HIV status, being faxed mistakenly to the patient's employer instead of the requested personal address. The location was discovered to have had a previous breach that had not been addressed by their compliance program.



COMPLIANCE ALERT

Brought to you by: Ethics, Compliance and Audit Services



[Audit](#) [Compliance](#) [Investigations](#) [Presidential Policies](#) [Contact](#)

[Fostering Medical Innovation: A Plan for Digital Health Devices](#)

The U.S. Food and Drug Administration (FDA) has created a new Digital Health Innovation Plan that will focus on fostering innovation in digital medical and health technologies. The plan also includes a post-market approach that aims to monitor and regulate digital medical devices. In the fall, the agency intends to pilot this new approach and provide guidance as to what types of digital devices and technologies are subject to comply with the FDA's policies.

Human Resources Compliance

[Education Department Memo Outlines Plans to Scale Back Civil-Rights Efforts](#)

Through a recent Department of Education memo, it was outlined that the Office of Civil Rights (OCR) would be applying a narrower scope when conducting investigations. Under the previous administration, complex investigations could broaden their scope and required three years of past data and information. The OCR has removed this requirement and will treat each complaint no different from another.

[Talk about Diverse Hiring Often Means Faculty. What about staff?](#)

A staff diversity program at the University of California at Berkeley aims to increase the number of minority staff in non-academic professional and management areas. Based upon UC's Women's Initiative for Professional Development, the program will provide participants skills to help them gain supervisory and managerial positions which have shown to have an underrepresentation of minority staff.

[UC Launches New Systemwide Procedures to Combat Sexual Harassment and Sexual Violence](#)

The University of California has introduced new procedures for faculty and staff to address and respond to alleged sexual misconduct at all UC locations. A similar procedure was introduced for students last year. The procedures remain consistent with the UC Policy on Sexual Violence and Sexual Harassment and provide several changes, including:

- Clear roles and responsibilities for Title IX offices.
- Processes for completing investigations.
- Added oversight over staff and faculty cases.

Research Compliance

[Updated Guidance on Executive Order Restricting Travel and Entry from 'Designated Countries'](#)

On June 26th, the Supreme Court issued a decision to allow portions of Executive Order 13780 to take effect. The order places travel restrictions to and from designated countries. In preparation for how UC students, faculty, scholars, and employees will be affected, the University has provided an updated guidance.

[When Misconduct Occurs, How Should Journals and Institutions Work Together?](#)

The Committee on Publication Ethics has drafted guidelines to address how research institutions and journals can work together to address research misconduct investigations and publication retractions. It is the aim of these guidelines to improve the communication between the two parties to ensure research integrity. However, it is acknowledged that the guidelines only serve as a start point for addressing differences.

[NYU Accidentally Exposed Military Code-Breaking Computer Project to Entire Internet](#)

Upon scanning the internet, a researcher discovered a New York University server maintained by the Institute for Mathematics and Advanced Supercomputing exposed confidential code-breaking information to the public.

[OFAC FAQs on President Trump's Cuba Announcement](#)

Announced on June 26, the current administration will reinstate certain travel and commercial restrictions against Cuba. In response, the Office of Foreign Assets Control (OFAC) has distributed a guide as it prepares to issue amendments to Cuban Assets Control Regulations in the following months.

[Notice of Extension of Effective Date for Final NIH Policy Requiring the use of a Single IRB for Multi-site Research](#)

The National Institutes of Health (NIH) has extended the effective date of this policy to January 25, 2018. Further guidance to assist organizations implementing the policy is available through the NIH's [Office of Science Policy webpage for IRB Review](#).

[Federal Science and Engineering Obligations to Universities and Colleges Declined 2% in FY 2015](#)

A report issued by the National Science Foundation compiles the number of obligations several federal agencies provided for use by academic institutions in the areas of science and engineering.



COMPLIANCE ALERT

Brought to you by: Ethics, Compliance and Audit Services



[Audit](#) [Compliance](#) [Investigations](#) [Presidential Policies](#) [Contact](#)

Policy

[New UC Policies](#)

[International Activities Policy:](#)

This is a new policy issued by the President of the University of California on June 23, 2017. The purpose of this policy is to: support international collaboration, education, exploration, research, and service; provide an administrative framework for international activities; and direct participants of international activities to consider and address potential risks.

[Recent UC Policy Updates](#)

[Guidelines on Acceptance of Personal Gifts and Gratuities by Employees under California's Political Reform Act:](#)

This guidance answers some of the most common questions regarding the receipt of personal gifts under the state Political Reform Act, in addition to providing a summarization of the law.

[Seismic Safety Policy:](#)

The purpose of this policy is, to the extent feasible by present earthquake engineering practice, to provide an acceptable level of earthquake safety for students, employees, and the public who occupy University Facilities and Leased Facilities. As of May 2017, this policy establishes a Seismic Advisory Board, implements a seismic risk model in lieu of interim use plans, and has been reformatted to meet web accessibility guidelines.

[Sustainable Practices:](#)

This policy establishes goals in nine areas of sustainable practices. Effective June 2017, this policy reflects the University Carbon Neutrality Initiative, includes the UC Green Laboratories Action Plan, and makes changes to the sections for Sustainable Building Operations for Campuses. In addition, the policy was remediated to meet web accessibility guidelines.

[PPSM 21: Selection and Appointment:](#)

This policy describes the process for selecting and appointing candidates for employment, including background checks, reference checks, and employment eligibility verification, as well as the employment of near relatives. As of July 2017, this policy has added language per Fair Employment and Housing Act (FEHA) regulation amendments and was revised to meet Web Content Accessibility Guidelines (WCAG).

Privacy

[Facebook Gets Slap on the Wrist from 2 European Privacy Regulators](#)

Investigations by Dutch and French authorities concluded that Facebook's collection of user information violated data protection rules in their respective countries. In their conclusions, the two European countries found the company did not sufficiently inform how user's could control the use of their data, violating privacy law.

[Google to Remove Medical Records Data from Search Results to Combat Leaks](#)

In order to provide greater privacy and remove potential personal information from its search engine, Google will begin removing all private medical records found in search results. Beforehand, Google only removed personal health information if it received a request for removal.

[Google Will No Longer Scan Gmail for Ad Targeting](#)

In order to appeal to corporate partners and create a uniform policy, Google will no longer scan emails for targeted advertising. Previously, privacy advocates had criticized the scanning practice conducted towards consumers using the free Gmail service. The company will continue to scan Gmail for potential security issues and advertise using information compiled from its other services.

[OU Shuts Down File Sharing Service After Failing to Protect Thousands of Students' Records](#)

Oklahoma University's newspaper, The Daily, discovered a file-sharing network exposed student records that included social security numbers, GPAs and grades, and financial aid information. According to the Family Educational Rights and Privacy Act (FERPA), students are given privacy protections. It appears that the unintentional breach resulted from incorrect privacy settings that allowed anyone with an ou.edu email address to search and find sensitive information in shared files.

[Border Patrol Says It's Barred From Searching Cloud Data on Phones](#)

When searching through U.S. traveler phones, border officers from Customs and Border Protection are not permitted to look at cloud stored data. This includes information stored only through apps, including email and social media. Content saved on devices are still subject to search without consent.