COMPLIANCE ALERT

Brought to you by: Ethics, Compliance and Audit Services

This Issue's Contents

Clery

The Need for Comprehensive Approaches to Campus Safety

Every year on October 1, colleges and universities are required to report on their campus crime statistics and security policies as required by the Jeanne Clery Act. Universities continue to contemplate organizational procedures for overcoming challenges to achieve Clery compliance.

Information on the Clery Act at UC campuses is available through the UCOP Campus Clery Act reporting webpage.

Cybersecurity

The 'Secure' Wi-Fi Standard has a Huge, Dangerous Flaw

A flaw in the encryption process for Wi-Fi Protected Access 2 (WPA2) networks would allow cybercriminals to attack and steal user data. Hackers would need to be within physical range of the vulnerable Wi-Fi network and some current device operating systems already prevent possible exposure. However, other Wi-Fi enabled devices will require a patch to once again secure the network.

NIST Special Publication 800-171 for Higher Education

With the deadline requiring organizations to comply with NIST Special Publication 800-171 approaching at the end of 2017, this guide describes the major areas affecting colleges, including potential barriers. Establishing a road map for managing the implementation of all NIST requirements will help higher education institutions meet compliance with the federal regulation.

Here's What's Happening at ECAS

♦ New Systemwide Director of Investigations

ECAS welcomes John Torres as the new Systemwide Director of Investigations at UC's Office of the President (UCOP). He has previous investigative and management experience through his work with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and the County of Los Angeles. The Office of the Director of Investigations is responsible for coordinating, tracking, and managing investigations at UCOP and systemwide, and maintains oversight of the university's Whistleblower policies.

♦ ECAS is currently recruiting for the position of Systemwide Director of Compliance. The Director of Compliance will be working with subject matter experts in Healthcare Compliance, Research Compliance, Export Control, and HIPAA/Privacy. Information for interested candidates was made available through the UCOP Online Job Posting.

♦ The UC Global Operations (UCGO) website is nearing its 1 year anniversary since launching December 2016. The website connects UC faculty, staff, students, and foreign collaborators with the information they need to navigate the complex world of international activities.

Information Security Program Assessment Tool

To continue to support higher education institutions with improving their information security programs, the Higher Education Information Security Council (HEISC) has provided a self-assessment tool mapping several frameworks, including the NIST Special Publications 800-171 and 800-53.

UNIVERSITY OF CALIFORNIA

COMPLIANCE ALERT

Brought to you by: Ethics, Compliance and Audit Services

<u>Audit</u>   <u>Compliance</u>   <u>Investigations</u>   <u>Presidential Policies</u>   <u>Contact</u>

Tips to Protect Your Information during the Holiday Online Shopping Season

Online shopping continues to grow in popularity. In 2016, for the first time ever, shoppers bought more online than in stores. And last year's Cyber Monday was the biggest online shopping day in the history of the US.

Unfortunately, the ease and convenience of online shopping makes the holiday season the perfect time for cybercriminals to take advantage of unsuspecting online shoppers. Three common ways that attackers take advantage of online shoppers are:

- Creating fraudulent sites and email messages
- Intercepting insecure transactions
- Targeting vulnerable computers

Fortunately, many cyber-threats are avoidable. When you shop in person, it's a habit to bring reusable bags, lock the car, and put away your cash or credit card when you're done with your purchase. Similar habits can protect you, your purchases, and your identity when you're shopping online during the holiday season and year-round:

1. Shop reliable websites, and get there safely.
2. Conduct research.
3. Always think twice before clicking on links or opening attachment. When in doubt, throw it out!
4. Keep clean machines!
5. Protect your passwords.
6. Check the address bar. Look for https:// (not http).
7. Check your credit card and bank statements regularly.
8. Get savvy about Wi-Fi hotspots and public computers.

Additional ways to protect yourself online:

- Choose your privacy and security settings; don't use defaults.
- If you wouldn't want your employer, landlord, professors, or grandma to see it, don't post it.
- Don't share info or pix about others that you wouldn't want shared about you.

Additional tips available on the <u>Information Security Website</u>.

Health Sciences Compliance

Office for Civil Rights Issues Guidance on How HIPAA Allows Information Sharing to Address the Opioid Crisis

In response to the declaration of a nationwide opioid crisis, the Department of Health and Human Services' Office for Civil Rights has issued guidance to healthcare providers describing how patient health information can be shared with close relations under certain circumstances. The guidance details how healthcare providers can proceed without violating HIPAA regulations, but continue to recognize patient autonomy.

Human Resources Compliance

Calling All Students: UC Wants Your Input on Sexual Violence and Prevention

The University of California is inviting students to apply for a seat on the inaugural student advisory board tasked with providing input on UC sexual harassment and sexual violence issues. Members will serve as liaisons to students on their campuses and help advise the university's systemwide Title IX office on its ongoing prevention and response efforts. Interested student may apply online by end of month, November 30 at 5pm.

Research Compliance

Additional Guidance on the NIH Single IRB Policy

The National Institutes of Health (NIH) has posted two guides to help institutions implement the NIH Policy on the Use of a Single Institutional Review Board (IRB) for Multi-Site Research. In addition, the NIH has posted a guide for organizations considering requesting an exception to the policy.

- Guidance on Exceptions to the NIH Single IRB Policy
- Guidance on Implementation of NIH Single IRB Policy

Ethics of Internet Research Trigger Scrutiny

With the increased use of public data for research, the possible existence of unintended consequences has begun to rise. Research integrity offices and universities in Europe are beginning to establish guidance to better define the application of ethical standards on internet research and using public data. The U.S. National Science Foundation has already begun a 4 year project to begin charting data-research ethics in an effort to produce guidance.

UNIVERSITY OF CALIFORNIA

Policy

Recent UC Policy Updates

BFB-G-28: Travel Regulations:

Revised 10/15/2017 to change the mileage reimbursement rate in accordance with IRS Notice 2016-79; revised language concerning payment of travel reimbursed by third parties; revised language on direct billing of rental cars. Clarified ancillary charges for airfare and base and economy fares. Provided a definition of state funds and referenced state law AB 1887. Revised the maximum daily meals and incidental reimbursement for CONUS travel under 30 days to $62 and instituted $275 dollar limit on daily lodging reimbursement in CONUS under 30 days. In addition, this policy was remediated to meet Web Content Accessibility Guidelines (WCAG) 2.0.

BFB-G-13: Policy and Regulations Governing Moving and Relocation:

This policy was reformatted to the revised template and has undergone minor technical corrections. In addition, it was revised to require submission of nontaxable expenses within a reasonable amount of time not to exceed sixty days. Added repayment provisions requiring new appointees to reimburse moving and relocation expenses if the appointees voluntarily separate from the position prior to completing one year of service. Removed policy on relocation allowances. Added policy on reimbursable sale of residence or unexpired lease expenses. Clarified the reimbursement of meals while in temporary living quarters. This policy was also remediated to meet Web Content Accessibility Guidelines (WCAG) 2.0.

PPSM-20: Recruitment and Promotion:

Policy changes effective as of October 23, 2017:

- Added the following sections: General; Scope; Competitive Recruitment Process; Career Appointments; Limited, Floater, and Per Diem Appointments; Contract Appointments; Documentation

- Added Internal Promotion

- Removed Career Ladder Recruitment and Required Procedures language

- Remediated to meet Web Content Accessibility Guidelines (WCAG) 2.0.

PPSM-22: Probationary Period:

The following revisions were made as of 10/31/17:

- Incorporation into this Policy of Personnel Policies for Staff Member (PPSM) 62 (Release During the Probationary Period or from Limited, Casual/Restricted, and Floater Positions).

- Clarification of existing definitions.

- Remediated to meet Web Content Accessibility Guidelines (WCAG) 2.0.

Privacy

Privacy or Accountability? Judges to Decide Which Prevails in Campus Sex-misconduct Cases

In North Carolina, advocates for the release of information concerning sexual misconduct cases at the University of North Carolina—Chapel Hill will appeal a court decision to allow the university to withhold information. The court decision referenced the FERPA federal law as taking precedence over state public records law.

New Research Details the Privacy Implications of Email Tracking

Researchers at Princeton University traced how email trackers can be used by third parties to reveal the online activities of users. The privacy-impacting features of several email providers were tested for how they successfully blocked proxies and trackers from revealing sensitive data.

14 Healthcare Privacy Incidents Reported in September

In September 2017, fourteen healthcare organizations reported breaches of patient health information. Included are academic medical centers and other public organizations that experienced phishing attacks, unauthorized access, and other compromises potentially leading to exposure of protected health information.

Privacy Breaches in University File System Affect 200 People

Stanford University's newspaper reported to University Officials that a campus file-sharing system revealed sensitive records on counseling sessions and confidential Clery related statistics and Office of Judicial Affairs emails. The information was accessible by any university member with Stanford log-in credentials. The university's Chief Privacy Officer has notified affected individuals of the potential privacy breach.

UNIVERSITY OF CALIFORNIA