The Bridge

A Joint University of California, Berkeley Publication of Audit and Advisory Services and the Office of Ethics, Risk, and Compliance Services

Volume 4, Issue 1 **May 2015**

Inside this issue:

6 Tips for Protecting Privacy at UCB

By Lisa Ho

Privacy is a hot topic, with massive personal data breaches and debate about government surveillance making the press almost daily. While the names in the headlines may be new, the stories are not. The University of California has long recognized privacy as an underpinning of academic freedom, and has sought to balance respect for privacy with transparency, accountability, legal responsibilities, and other obligations.

Because the ability to amass, analyze, and access personal data has expanded exponentially with today's technology, our everyday activities have a major impact on privacy. Protect your own privacy and the personal information of others by incorporating these tips into your daily practices.

1. **Separate personal and business email**

What to do

- Send and receive personal messages using a personal (non-University) email account. Conversely, conduct University business using a berkeley.edu account.
- Delete personal messages from your Berkeley account (forward them first to a personal account if you wish) or, at a minimum, move personal messages to a folder labeled "Personal."

Why?

UC policy* has strong email privacy protections, but there are multiple situations that require disclosure of email (given appropriate approvals), e.g., Public Records Act requests, legal proceedings, internal investigations, and business continuity. Only keep personal mail in your account that you are comfortable having others view.

On the other hand, if you use your personal account for business, you may be obligated to hand over email from that account in the above situations. So, in this context, work/life balance means keeping personal and business correspondence in separate buckets on opposite ends of the scale.

2. **Use Departmental Accounts (SPA)**

What to do

- If you have a Departmental Account (aka **Special Purpose Account** or **SPA**) for your unit, use it for any correspondence and documents that someone would need to continue your work (for example, in case of unexpected medical leave) or for reference documentation.
- Publicize the SPA address, send messages from it, cc it on relevant correspondence, forward messages to it.
- Make the SPA the account owner of non-transitory documents that have ongoing value. (For bDrive, first share the file with the SPA account, then make the SPA the owner.)
- If you do not yet have a SPA, look for announcements in the coming weeks about expansion of the SPA pilot with self-service SPA creation.

(Continued on page 2)

6 Tips for Protecting Privacy at UCB

(Continued from page 1)

Why?
SPAs do not get deleted when an individual leaves the University. If information needed for business continuity is available in a SPA, access to your individual account will not be necessary when you are not available.

3. Get consent or approval before accessing data

What to do
- If you need access to an individual's email account or computing device, first get consent (written when possible).
- If you cannot get consent, contact the UC Berkeley Privacy Office for help BEFORE taking action.

Why?
UC policy requires consent before looking at an individual's files or email, or approval from specific campus officials when you cannot get consent. Additionally, access without consent is limited to "least perusal necessary" so having personal mail clearly marked as such creates a layer of separation.

4. Employee separation: Remove personal data

What to do
- Before an employee leaves the University, designate time for the employee to: 1) delete personal information from University devices and accounts and 2) move documents and correspondence of ongoing value to a SPA.
- Have the employee document in writing that personal information has been removed from University devices and accounts.
- Establish privacy expectations with new hires and current employees (share this list!) for smoother separation processes in the future.

Why?
Avoid the need to access individual accounts.
Minimize privacy intrusions when access is required.

5. Consider Privacy in Contracts/Partnerships

What to do
- Engage procurement or other contract offices early in the negotiation process for help with privacy in contracts.
- Think through potential privacy risks when engaging with suppliers or partners working with University data.
- Use caution with free and low cost services.

Why?
Just as we care about protecting privacy within the institution, we need to ensure privacy protections from suppliers doing work on our behalf. Most free and low cost services do not provide appropriate protections for sensitive data.

6. Look out for the "forbidden five"

What to do
Remember these five data types:
- Social Security Numbers
- Credit card numbers or other financial account numbers
- Drivers License or CA ID Card numbers
- Health information
- Health insurance information

If you see them ask (yourself, your manager, the Privacy Office, or Information Security and Policy) whether they are being appropriately protected. They are not forbidden, but they require special handling.

This is not an exhaustive list of data that require elevated protections, but these are the most likely to be encountered across campus.

Why?
Some types of data require elevated protections because of the high negative impact if inappropriately disclosed.

Finally, if you have privacy questions or concerns, contact the Campus Privacy Officer, in the Office of Ethics, Risk and Compliance: Lisa Ho, 510-664-7775, privacyoffice@berkeley.edu, or visit http://privacy.berkeley.edu.

**Electronic Communications Policy http://policy.ucop.edu/doc/7000470/ElectronicCommunications*

Identity Fraud Prevention and Response

By Barbara VanCleave Smith

Just as UC Berkeley strives to prevent identity theft, we also strive to prevent identity fraud. Fraud is a false representation of a matter of fact intended to deceive another. So, identity fraud is fraud committed or attempted using the identifying information of another person without authority.

Identity *fraud* follows identity *theft*: first someone steals another individual's personal information, then tries to use that stolen personal information to obtain money, goods, or other advantages. The theft might have occurred years in the past and/or thousands of miles away. Identity fraud could occur anywhere on campus, to any member of our campus community.

Since 2010, UC Berkeley's policy on *Identity Fraud Prevention and Response* has required units to explicitly look for so-called "red flags" indicating possible identity fraud. A red flag is a pattern, practice, or specific activity that indicates the possible existence of identity fraud.

The following are examples of common red flags that may indicate that an individual's identity has be compromised:

A. Suspicious documents
- An identification document or card that appears to be forged, altered, or inauthentic.
- An identification document or card on which a person's photograph or physical description is inconsistent with the person presenting the document.
- A document with information inconsistent with account holder information on file.

B. Suspicious personal identifying information
- Identifying information inconsistent with other information provided by the account holder (example: inconsistent birth dates or a different address).
- Identifying information typical of fraudulent activity (such as an invalid phone number or non-existent billing address).
- Social security number the same as that of another person.
- Address or phone number the same as that of another person.

C. Suspicious account activity or unusual use of an account
- Change of address for an account followed by a request to change the account holder's name.
- Payment stop on an otherwise consistently up-to-date account.
- Account used in a way that is not consistent with prior use.
- Mail to the account holder repeatedly returned as undeliverable.
- The account holder reports to the campus that he or she is no longer receiving mail sent by the campus.
- Notice to the campus that an account has unauthorized activity.
- Breach in the campus computer system security.
- Unauthorized access to or use of account information.

D. Notifications and warnings from credit reporting agencies or others

A red flag does not automatically mean that identity fraud is being attempted. Campus personnel who detect red flags must take one or more of the following steps, depending on the degree of risk posed by the red flag:

- Request additional documentation to validate identity;
- Contact the account holder or applicant;
- Change passwords or other security features that permit access to the account;
- Not open a new account;
- Close an existing account;
- Provide the account holder with a new student or staff identification number;
- Notify the program administrator for determination of the appropriate step(s) to take;
- Notify the UC Police Department;
- File or assist in filing a Suspicious Activities Report (SAR) with Risk Services (risk@berkeley.edu) in the Office of Ethics, Risk and Compliance Services; or
- Determine that no response is warranted under the circumstances.

For more information, see the UC Berkeley policy on "Identity Fraud Prevention and Response" at http://campuspol.berkeley.edu/policies/IdentityFraud.pdf.

Public Records and Not So Private Components

By LeVale Simpson

Under the California Constitution the University of California is uniquely positioned as an autonomous public trust. However, for purposes of the California Public Records Act (CPRA), the University is a state agency and subject to CPRA's governing provisions. Aside from specific, limited exceptions, CPRA requires that the University release to any member of the public any records "prepared, owned, used, or retained" by the University (California Government Code §§ 6250 et seq.). In essence, most University documents are subject to release under CPRA. Yes, that includes -- but certainly is not limited to -- email correspondence, employment contracts with terms of compensation, and meeting minutes.

Of course, there are exceptions to the general rule that most University documents are subject to release. In those circumstances, the Public Records Office will redact responsive records where appropriate, or withhold records in their entirety if the exempt portion contained within the record cannot be reasonably segregated . Most of CPRA's exceptions are found under California Government Code § 6254. The exceptions we most commonly encounter are as follows:

University officials should proceed as if everything "prepared, owned, used, or retained" by the University is public,

- Records pertaining to pending litigation to which the University is a party are exempt from release until the pending litigation has been finally adjudicated;
- Personnel or medical records, the disclosure of which would constitute an unwarranted invasion of personal privacy, are exempt from release. Under this particular provision, University officials' (i.e., all employees) individual employment files are generally exempt from release. However, certain records contained within those files may be subject to release (e.g., employment contracts with terms of compensation).
- Test questions, scoring keys, and other examination data.
- Records prohibited from disclosure under federal or state law. The California Evidence Code, for example, exempts the disclosure of attorney-client privileged communications, so pursuant to 6254(k) such records are also exempt from release under CPRA. Family Educational Rights and Privacy Act (FERPA) and HIPAA (Health Insurance Portability and Accountability Act (HIPAA) protected records are also exempt pursuant to this provision.

The above exceptions seem straightforward enough; however, difficulties can arise in determining whether certain exceptions apply to particular records. As one might imagine, the types of records that are typically requested do not always fall into neat categories and there can be significant gray areas. What's more, there are misconceptions among University officials as to what is or is not subject to release. Returning to our attorney-client privileged communications example above, some University officials have an inaccurate belief that marking sensitive documents "Confidential" or "Attorney-Client Privileged" is enough to protect those documents from CPRA disclosure. Marking documents "Confidential" has no bearing on whether those records will be subject to release under CPRA. Generally, documents identified as "Attorney-Client Privileged" are only withheld from disclosure if those records actually relate to legal advice being sought or rendered. Of course, this all requires discretion and reasonableness. The California Public Records Act should not hinder officials' ability to work effectively and with some degree of candor, but it is important to balance those with an understanding that the University is a public institution.

Please visit the Public Records Office's website (http://chancellor.berkeley.edu/services/public-records) for contact and additional information.

Takeaways

- University officials should proceed as if everything "prepared, owned, used, or retained" by the University is public, and may one day be a part of a public records request.
- Consider what you have written in an email before hitting the send button.
- Regularly purge unnecessary or duplicative email correspondence in accordance with the University retention policies.
- Consider whether it is necessary to retain multiple drafts or iterations.
- Remember that "Confidential" is not some magic word.

Audit Cables: Tips for Avoiding Social Media Pitfalls

By Chad Edwards

Align social media and department strategy

Understanding your organizational strategy, what is your primary goal for being socially active? Create awareness? Increase enrollment/participation? Generate revenue? Receive feedback? The true value of social media lies in its effective use to humanize the organization appealing to and persuading people to behave in a manner that furthers mission attainment. To successfully align the use of social media with the organizational strategy, consider the following.

- Understand your goals and objectives, including your products or services.
- Gain an understanding of your target audience or customers, their needs and expectations around engagement.
- Evaluate whether the use of social media will enhance strategy achievement and fit with the target audience profile.
- If yes, develop a social media channel plan. Different channels are better suited for certain goals and audiences.
- Establish performance metrics upfront that are tied to the organizational strategy.
- Finally, execute the plan and manage the investment by monitoring performance and adapting accordingly.

Counter cybersecurity risks

Social networking is built upon mutual trust. Attackers seek to exploit this trust relationship to damage reputations, disrupt operations, or for financial gain. Their tactics include taking control of social media sites and posting links to websites controlled by them to distribute malware or exploit vulnerabilities in web browsers, web browser extensions or applications. As a precaution, use strong passwords (https://security.berkeley.edu/content/passphrase-complexity), avoid re-using passwords for other sites, and where available use two-factor authentication. Hover over links and look at statistics bar at the bottom of your browser to see where the link goes before clicking on it. Install software security patches within 48 hours. Lastly, prepare an incident response plan to expeditiously identify, contain, eradicate, and recover from incidents.

Think twice before posting

Understand the boundaries between speaking on behalf of the University and yourself personally. There are many examples of the individual who wished they could retract a post. Social media moves at an exponential pace when compared to other communication channels. Abstain from conversation likely to compromise the privacy of others; for example, be mindful of compliance obligations under the Family Educational Rights and Privacy Act (FERPA). Refrain from conversations that may create the appearance of lobbying, resemble hate speech or is otherwise offensive, or be construed as of an endorsement, promotion, or recommendation.




Announcements

New International Risk Website

Risk Services created an International Risk website for members of the campus community. The homepage answers common questions and provides emergency updates (such as calls for evacuation from countries in crisis). Links to individual countries inform the campus community about personal safety, compliance, and legal and political climate. The site is a work in progress. Entries for the campus's most visited countries are complete, but less-visited countries may not be completed for a few months. We invite you to visit the site and let us know if you have any suggestions for improving it! The web site can be found by going to http://riskservices.berkeley.edu/international-risk.

RISK SUMMIT

The University of California's annual Risk Summit will take place on June 4 and 5 at the Downtown Oakland Marriott, which is easily accessible by BART (take the Downtown Berkeley station to Oakland-12th Street). There is no charge for University employees to participate. This year, the Risk Summit is highlighting eight different tracks:

1. Collaborating Toward Risk Mitigation
2. Cyber Risk
3. Environment, Health & Safety
4. Emerging Risk
5. Enterprise Risk Management
6. Hospital and Professional Liability
7. Human Capital

Student Life and Health

If you work in any these areas, or just have a strong interest in one of them, we encourage you to attend! You may register for the Risk Summit by going to http://www.ucop.edu/risk-services/ files/RS2015-At-A-Glance-04132015.pdf.

Contact Information

Audit and Advisory Services
611 University Hall MC 1170
Berkeley, CA 94720-1170
Phone: 510-642-8292
E-mail: audit@berkeley.edu
http://audit.berkeley.edu/

Do you have a question for Audit and Advisory Services? Please e-mail it to audit@berkeley.edu

or submit it online at:

http://audit.berkeley.edu/services/ask-auditor/submit-your-question.

Office of Ethics, Risk and Compliance Services
2130 Center Street, Suite 200 MC 4208
Berkeley, CA 94720-4208
Phone: 510-642-5141
Fax: 510-643-0281
Email: risk@berkeley.edu