UC SANTA BARBARA POLICY AND PROCEDURE

Guidelines Concerning Click-Through Agreements
Contact: Policy Office - Administrative Services; Information Security - Enterprise Technology Services; Procurement Services - Administrative Services
Issued: June 10, 2015
Pages: 3

GUIDELINES CONCERNING CLICK-THROUGH AGREEMENTS

I. INTRODUCTION

"Non-UC technology services" are computer-related services offered online, often for free or at low cost, for which there is no UCSB or UC system-wide agreement. These services can take many forms, including non-work Google accounts; data stored in Apple or Microsoft's cloud service or with an online backup service; photos shared with Flickr and Picassa; Dropbox and iCloud used to store, move, and share documents; Skype and instant messaging (IM) to stay in touch with others; thoughts shared on Facebook, Twitter, and Instagram; and the list goes on.

Prior to using non-UC technology services, it is essential that you consider the risks associated with the service. It is important to remember that when you use these services in connection with UC business, your data -- the University's data -- is in someone else's hands. Non-UC technology services typically require acceptance of "click-through" agreements that have not been reviewed or approved by UC's Office of General Counsel (OGC) and that might include terms and conditions that UC cannot accept. A contract executed by anyone other than someone with delegated Signature Authority may be **considered unenforceable** because Implied Authority is inapplicable at the UC. Therefore, if you accept the terms of a click-through agreement without first consulting Procurement Services, it is possible you may be held personally responsible for the terms of the agreement.

UC and UCSB privacy and security policies apply to all University data, whether it is housed on UC or non-UC systems, and the terms and conditions of many click-through agreements may conflict with these privacy and security policies. These click-through terms and conditions also typically conflict with UC's requirements regarding indemnification obligations, apportionment of damages, limitations of liability, use of the University's name and marks, and litigation venue. Each of these issues must be carefully considered when determining whether to use non-UC technology services.

II. THE BOTTOM LINE: THINK BEFORE YOU CLICK

A UC-approved service agreement is **required** for non-UC technology services involving the storage, receipt, processing or publishing of Restricted and Confidential Information on non-UC systems. An individual who uses a non-UC technology to process or store restricted or confidential information may be held responsible in the case of a data security incident and could possibly be subject to discipline. "Restricted Information" is defined in Business and Financial Bulletin (BFB) IS-2 as any confidential or personal information that is protected by law or policy that requires the highest level of security protection, whether in storage or in transit. "Restricted information" includes but is not limited to: personally identifiable information (PII); notice triggering information; PCI Data; and contractually protected data. "Confidential Information" is categorized in Business and Financial Bulletin (BFB) IS-2 as information for which unauthorized access to or disclosure could result in a serious adverse effect, cause financial loss, cause damage to the University's reputation and loss of confidence or public standing, or adversely affect a partner. To ensure compliance with these requirements, you must work with Procurement Services to establish a service agreement employing UC-approved terms and conditions addressing information security and privacy requirements, including encryption.

Do not use a non-UC technology service without a UC-approved agreement if any of the following apply:

- Restricted or Confidential Information will be involved;
- You will be conducting University business that should not be disclosed to the general public;
- You need a high level of security;
- Privacy is a concern;
- There are things that wouldn't be OK for the service provider to do with the University's information;
- The University information is subject to export control laws that might be violated by international storage;
- You have specific requirements for availability of data and electronic communications that the service can't guarantee;

- It would be a problem if the service suddenly changes or is no longer available, either temporarily or permanently.

If any of the above applies, consider whether the University offers a solution you could use instead. It is important to remember these considerations throughout the business relationship with the service, not just at the beginning, as your use of the service could change over time. An ETS Business Relationship Manager may help. If not, work with Procurement Services to consider the range of vendor options and establish a UC-approved agreement before engaging a vendor's service or system solution.

III. PROTECTING PRIVACY

Keep in mind that your privacy, and the privacy of everyone using the free/low cost application or service, is dependent on the service provider. Don't assume that privacy, security, or business continuity protections will meet UC's standards.

- **Don't use external information systems or services for anything that you're not prepared to disclose or lose.** It is best to assume that whatever information goes to or through the service may become public. This includes records of activities of those using the service, such as who used the service, what they used it for and when, etc.
- **Check out the company's privacy policy.** There should be a link to it somewhere on their website. Know what the vendor is going to do with the information you and others provide. This includes who they may provide information to and who they will allow to access it. What permissions have you granted by accepting their agreement/Terms of Use?
- **Don't use non-UC information systems or services to collect personal information.** California law requires compliance with the California Information Practices agency requirements (see CA Civil Code 1798.14-1798.23) and such compliance cannot be ensured if non-UC systems are used.
- **Don't expect to be informed if a subpoena, search warrant or other legal instrument is presented to the company to obtain information about you or others using the service.** This is true even if a UC-approved agreement is in place. While some organizations will try to direct the agency serving the notice to you or the University, there is no guarantee that this will happen. In some cases the vendor may be forbidden from disclosing the request.

IV. OPERATIONAL, LEGAL, AND CONTRACTUAL ISSUES

Also consider the following when evaluating whether a specific free/low cost service is the appropriate solution for your needs:

- **Contracts:** When you sign up to use free/low cost services, you may be agreeing to terms and conditions, terms of service, and acceptable use policies that are different from UCSB's or UC's. A contract executed by anyone other than someone with delegated Signature Authority may be considered unenforceable. It is possible that the company could hold you personally to what you agree to, even if it is just a "click-to-accept"-type agreement. Also, if the service is free or "click wrap" you will probably have little or no recourse against the vendor if something goes wrong or they do something you don't agree with.
- **Ownership:** It is essential to ensure that University data remains the property of the University. Whenever you put data on a commercial service, ensure that the terms do not conflict with University policy in terms of data ownership.
- **Availability of Data:** Don't expect to get your information back if the company has a disruption in service, is acquired, changes business models or goes out of business. Keep local copies/backups of any critical data or records just to be safe.
- **Record Requests:** Keep in mind that you may be **required** to produce records relating to University business, including email, instant messages, files, etc., regardless of whether those records are stored on University or non-University systems or services. Using a non-UC service may make it more difficult for you to comply.
- **Deleting data and accounts:** There is no guarantee that deleted content or accounts will really be deleted. It may take a while before the content or the account is completely flushed from all of the company's archives. Practices will also vary as to how long accounts may remain idle before the account and associated data are destroyed.
- **Accessibility:** If use of an application or service will be required, e.g., the only way people can access your online content, complete an assignment, or respond to a request for information, you must make sure that it is accessible to users with disabilities. Ask the vendor whether their product is compliant with Section 508 of the U.S. Rehabilitation Act, and test it to make sure that it is. More information about web accessibility and testing web sites for accessibility can be found at UC's Electronic Accessibility website (http://www.ucop.edu/electronic-accessibility/).

V. UCSB REQUIREMENTS RELATING TO THE USE OF WEB ANALYSIS TOOLS

All web pages that use third-party (non-UC) web analysis tools, such as Google Analytics, must link to:

UCSB's "University of California, Santa Barbara Privacy Notification Statement" web page at: http://www.policy.ucsb.edu/privacy-notification/.

Google Analytics (GA) account administrators must configure GA not to share GA data, so that the usage statistics will only be available for UCSB's local use. (Account admins: for each GA account, check “Do not share my Google Analytics data” on the “Edit Account and Data Sharing Settings” screen.)

VI. CONTACTS FOR ASSISTANCE

If you need assistance in this area, please contact:

- Procurement Services, Business and Financial Services
- Information Security, Enterprise Technology Services