CLOUD COMPUTING CONTRACT TERMS

Accessibility/ADA
Consideration or care should be given to users with disabilities and solutions should be ADA compliant. Cloud solutions should not deprive disabled people experiences and/or functionality similar to non-disabled people.

Audits
There are industry standards for information security management and for reporting on the controls in a service organization. The contract should indicate that the service organization is certified as compliant with (1) ISO 27001 (which specifies explicit information security management controls) and with Statement of Standards for Attestation Engagements (SSAE) No. 16 (a regulation defining how service companies report on compliance controls). Audits, which should be performed annually and immediately following any Security Incident, disclose the controls, processes and safeguards that are in place for customer data. They also provide reports on internal controls over any financial reporting.

Business Continuity & Disaster Recovery
Business Continuity and Disaster Recovery are critical if you must have uninterrupted access to a service. The contract should outline the Vendor's responsibilities for providing uninterrupted service. The contract should provide information on the Disaster Recovery/Business Continuity plan; how will the vendor keep business going while it recovers from an unexpected event?

Ask if Vendor will prorate fees for any disruption to service.

Data Location
Some Vendors reserve the right to store customer data in any country in which they do business. There may be Export Control issues if research data in particular is stored outside of the United States. Ask if the data will be stored exclusively in the U.S. Under any circumstance, be sure the contract identifies where the data will reside.

Data Privacy
Contracts should clearly state that the vendor will not share personal data with anyone, and that the vendor will do only what Princeton University permits them to. Contracts should require that all Princeton University's data be kept confidential.

Data Recovery
The contract should state Princeton University's rights to access its data, and it should be clear on the process by which data will be returned or retrieved if the contract is terminated. The process should
include a timeline and a format for the data. The vendor should be obligated to securely destroy any of Princeton University's data at an agreed upon date after termination of the contract.

*Most vendors will not stipulate their data recovery plans in a standard contract. You may request to see their plans or include a provision about acceptable time & costs in the contract.*

**Data Retention**
A Vendor's obligation to retain data may depend on the amount of data and/or the length of time that the data is stored. The vendor may offer archiving services, for a charge. Be sure to understand how much data may be stored and for how long without incurring additional cost.

**Data Security and Facilities**
Vendor contracts will provide some level of security for your data (e.g. "industry standard") but it is best to specify a security standard. For certain kinds of data (such as HIPAA) there may be specific security requirements that must be included in the contract. Regarding the facilities housing your data, verify the specific infrastructure, as well as the security procedures in place; physical security as well as encryption, firewalls, etc.

*Consult with University's IT Security Officer or the Architecture Review Board. Explore using CAS or similar authentication architecture.*

**Data Transfer/Storage**
Encryption is used to protect the confidentiality of data being transferred over networks. Data must be encrypted when it is transferred across the internet. However, it is optimal to also have the data encrypted when it is "at rest" and stored on hard drives.

**Family Educational Rights and Privacy Act (FERPA)**
FERPA deals with the privacy of student records. Vendor contracts should allocate responsibility and liability for maintaining that privacy. The contract must convey that the vendor/service provider is a "School Official" with a "legitimate educational interest" in any of our data that is protected by FERPA, and that they will comply with the regulations on behalf of Princeton University. It should also specify responsibilities in the event of a data breach.

*Contractually require that vendors notify you if a data breach or unauthorized data access has occurred and request details regarding what corrective measures have been taken to mitigate the risk and prevent re-occurrence.*

**Health Insurance Portability and Accountability Act (HIPPA)**
HIPAA requires the protection and confidential handling of protected health information. Specific security controls are required when there is electronic transfer of HIPAA information.
If your business needs require you to store HIPAA protected information in the cloud, please consult with the Office of General Counsel.

**Information Types**
Certain types of information are particularly sensitive. These include but are not limited to:
- Personally Identifiable Information (PII): Date of birth, Social Security Numbers
- Credit card information
- Usernames, PINS, passwords and related security questions

*While it may be necessary to collect and or store PII, extreme precaution should be taken to limit access to such information on a strict need to know basis. Verify that web crawlers and other tools do not have access to these types of information.*

**Legal Holds and Access to Data**
The contract should specify the Vendor’s obligations if any data becomes the subject of a subpoena or other legal or government request for access.

**Location of Data**
There may be concerns or implications if data is stored outside of the United States. Different countries have different laws pertaining to data. The contract should identify where data will reside. If outside the U.S., question whether that is an issue of concern.

**Notifications when something changes**
Cloud computing contracts often reserve the right for the vendor to unilaterally make modifications to the services or to the URL terms of service.

*Ask to include a qualification prohibiting "materially detrimental" modifications. This will not guarantee that all modifications are beneficial but will provide at least some protection against changes that may be unfavorable.*

**Ownership of Data**
It is important to establish that Princeton University is the owner of any data that resides in a cloud infrastructure. The contract should clearly state that Princeton owns all rights, title and interest (including intellectual property rights) to the data.

**Price Cap**
Price cap on annual maintenance or subscription price increases.

*Ask the vendor if the contract can include a cap on annual price increases.*

**Security Breach**
The contract should spell out what the vendor’s specific responsibilities are in the event that data is accessed inappropriately. There are explicit obligations if Personally Identifiable Information (PII) is involved. The contract should also require the vendor to indemnify Princeton should data be accessed inappropriately.

*Identify the process for vendor to use in addressing a breach.*

**Service Level Agreements (SLA) and Performance Monitoring**

SLAs are agreements that typically quantify what service will be provided. It is used primarily as a gauge for a vendor’s responsiveness to a support need. While SLAs are good for resolving problems, or keeping service running, the service may be running at deprecated level making the use of the application impractical. To mitigate such instances, performance monitoring stipulations can be included in a contract.

*Contracts should stipulate:*
  - **guaranteed uptime**
  - **penalties for non-performance**
  - **notification of scheduled maintenance**
  - **response time guarantees**

**Suspension of Service**

Services may be suspended by a vendor for several reasons (e.g. end user violates use policies or payment for a service is overdue). Make sure you understand the circumstances under which the vendor is allowed to suspend service and the necessary steps preceding any such suspension.

**Termination**

Be sure to clearly define terms under which the contract may be terminated. In many cloud computing contracts, the customer may terminate at will; ask for contract to stipulate the right to “terminate at will”. Regarding the Vendor’s right to terminate, be sure it includes adequate notice to allow Princeton to secure a suitable alternative vendor.

*Make sure it is clear how Princeton will retrieve its data, including the format, and any costs to migrate the data to a new location.*

*The contract should obligate the vendor to securely delete data from their system (including backups) after Princeton has retrieved all of its data.*

**Use of Customer Data**

Customer data can be defined as information about the purchaser of a service, or its customers. Cloud service vendors can harvest details such as names, addresses, phone numbers, demographical information and purchasing patterns directly or indirectly from visitors to a website. This information can then be used by the cloud service vendor to sell products and services, or this information can be resold to another company. Carefully review and evaluate whether there are any uses of Customer Data contemplated by the vendor, seek necessary limitations and consult with General Counsel if necessary.
Look for targeted ads (ads that rely on browsing history, previous purchases, and demographics). In some cases, a vendor will use banners or exit pages to advertise to users of your application, some vendors may even provide financial incentives for you to participate.

Look for conditions that allow the vendor to use contact information for direct mail, email and phone to sell product

For further information contact:
Becky Goodman
OIT, Operations & Planning
Last Updated: December 10, 2013