**Cloud Computing Checklist**

**Key Questions**

* Where does the data fall in your institution's data classification?
* Is the data regulated (PCI, HIPAA)? **If yes, compliance is mandatory, not optional**

**Privacy/Confidentiality**

* Where does the data fall in our data classification?
	+ They have to meet our requirements and regulatory requirements (i.e., PCI, HIPAA, etc.)
	+ Classify the data.
	+ Not all cloud/third party services will need the same level of scrutiny.

* Some require us to monitor the security situation, so make sure we get the right to do this if necessary. Make sure monitoring is on-going and not just a onetime thing.

* Clarify privacy responsibilities for the vendor. Under what circumstances may they release our data?

**Data Security and data breach responsibilities**

* Require them to promptly disclose per Wisconsin law, not their laws.
	+ WI law applies, regardless of where THEY are housing our stuff.
	+ What about more stringent laws like Massachusetts? We’re on the hook for their students here!

* Make the breach their problem in the contract.

**E-discovery**

* Know what you have and how to get it. Make sure the contract allows for this.

* Will we be charged for ediscovery request fulfillment for data that lies outside the boundaries of our usually accessible information? For example, transactional data such as IP, date and time.

**Patent infringement**

* Users of infringement patent can be sued along with the actual offender. Negotiate a warranty that prevents this in case they are sued for stealing someone else’s code. Make sure they own what they are selling you.

**Incorporated URL terms that are modifiable at will**

* They shouldn't be able to change any part of the agreement without your approval. This is very common, especially for their "EULA" portion.

**Responsibility for end users**

* Make sure the contract indicates that the Institution will use “reasonable efforts” or will notify users of their obligations. Whatever you do, don’t agree to be totally liable for what your users do.

**Export Controls**

* Google Apps EULA allows for them to store stuff anywhere, including China, which could cause us to violate export control laws. Mandate that ours has to be stored here or in a non-export controlled place.

**Business Continuity/SLA**

* How much uptime do you need (24x7 or less)? Get specific about this.

* What’s the penalty if the uptime is not met? Money back? Ability to leave the contract?

* Determine whose job it is to patch the OS and applications and get that in writing.

* Determine performance requirements as well in terms of end user experience.

**Suspension/Termination and their aftermath**

* What if they go out of business or the contract is otherwise voided/cancelled? Who owns the data? If it’s a free service, are they putting language in here removing your rights?
	+ Define what you expect. Transfer of data back to us and secure destruction?
	+ Define format of data (csv for ex.).
	+ What data? Metadata too? Not just a pile of 0’s and 1’s.
	+ What would it take to get the SERVICE going somewhere else?

* How fast and for what reasons can a vendor terminate services?
	+ Will you have time to transition to another vendor?
	+ Will you have access to your data? If so, in what format and for how long?

**Warranties (or lack thereof)**

* Make sure the contract includes warranties against patent infringement and data breaches. Don’t take on the risk of THEIR business.

**Indemnification (both ways)**

* Make sure the contract ensures no third party lawsuits. So if someone sues us for something done with Pantherfile, Xythos is safe. The other way, someone sues Qualtrics for a data breach, not our bad. Ensure this runs BOTH ways.

**Choice of law and jurisdiction**

* Any lawsuit filed has to be filed in the defendant’s jurisdiction.

**Data Segregation**

* Ensure there is proper separation between us and other clients, especially for cloud computing environments (both data in storage and network traffic attacks). Define what our recourse is if another customer gets unauthorized access to our data.

* Commingling or combining of data. Can they tease out our data if we leave the contract? Can other customers get at our stuff? If it’s on the same disks, could they sue for the disks and get our stuff too?

* Ensure that they are not allowed to use a snapshot of our Platform as a Service (PaaS) for another customer (data leak concerns).

* Conversely, ensure that they are responsible for the security of any OS's snapshots they've obtained from third parties.

**Data Mining**

* Watch out for “Free” data mining. They usually do this for free to get at data or metadata for marketing or other information of value.

* Understand any secondary uses of data by the cloud provider and develop language in the contract to prohibit them if necessary/desirable.
	+ May need to have data mining expressly prohibited, if necessary. However, if this is no big deal, then great, we get something for free. Evaluate accordingly.

**Third party contracts**

* Do they have a third party providing storage or networking?

* Make sure they are holding THEIR third party sub-contractors to adequate technical, physical and organizational security measures.
* Make sure they have a program to verify that all third parties they use are compliant with applicable regulations (i.e., PCI, HIPAA, etc.)

**Specific Security Controls**

* May want to require specific controls such as encryption, firewalls, least access, silos based on how confidential the data is. The more you need, the more it will cost you.

* Require a Type II SAS70 or include a right to audit clause in the contract. The SAS 70 Type II report must apply to the environment and application being proposed and include at least the following areas:
	+ Physical access to the equipment housing the application and data backups
	+ Security Administration procedures for the application and operating system environment.
	+ Logical access controls for the application and operating system environment.
	+ Network security including firewalls, patch maintenance and incident response to breaches, virus and other attacks.
	+ System Development and Maintenance procedures including application change management procedures and audit tracking of all changes.
	+ Application, operating system and network security monitoring procedures.
	+ Daily database backup procedures
	+ Written recovery plan of the PSOA database and infrastructure environment
	+ User control considerations

If a SAS70 Type II is not provided, the vendor must provide a written description of the above information.

* Consider asking for evidence of their information security program including administrative, technical and physical security measures.

* Consider requiring evidence of compliance with an accepted security standard such as ISO for any cloud contract involving confidential data.
* For web applications, ask about testing against the OWASP standards.

* For credit card data, insist on all applicable PCI compliance certifications and details of what PCI compliance issues are yours and which are their responsibility.

* For HIPAA data, insist on HIPAA compliance certification and make HIPAA compliance their problem in the contract for aspects of that which are under their control.

* If using for confidential data, inquire about their HR policies. Do they do background checks? Even if the data is physically stored in the US, do they farm out services from foreign countries? Is this okay?

* Define log/access monitoring roles and requirements.

**Backups/recovery**

* This is their problem if they are hosting the data unless it's something we cause.

* Recovery expectations should be defined in the SLA

**Identity/Access Management**

* Consider requiring InCommon as a standard for Software as a Services (SaaS) and other hosted services where we'll be using our campus ID's to log in.

* Ensure that login communication is always encrypted.

* In general, ask for security assurance for interfaces/API's

*Checklist created and maintained by Steve Brukbacher, University of Wisconsin-Milwaukee (UWM), with the assistance of the UWM Office of Legal Affairs, UWM Internal Audit and University of Wisconsin System Purchasing.*

*Last revised Oct. 6, 2010*