SUNY Campuses and Cloud Storage

A GUIDANCE DOCUMENT

Prepared by the SUNY Compliance Office and the Records Management Officer
February 2016

Table of Contents

What is Cloud Computing

Cloud computing in simple terms is using an outside service provider to store manage and process our data. The reason this service is referred to as "the cloud" is that you never truly know where your data is physically stored. Examples of cloud computing include creating documents on google drive, sharing files via dropbox, or storing music or pictures on Apples icloud drive, or Amazon Prime's Cloud drive.

Note that there is a difference between cloud computing hosted by your institution and cloud computing hosted by a third party. With the latter, where a third party vendor is providing the cloud service, an institution will have to follow more steps to ensure the safety of their data, since it will be in the possession of a third party.

SUNY Campuses and Cloud Services

When it comes to cloud storage, or any contracts for information security and technology services, the best advice, and best practice, is to make sure any contract or agreement for the service goes through Counsel's Office (and the specific campus attorney) for review and approval.

The most important considerations for an institution looking into cloud services are privacy and security - keeping the information we possess private, and ensuring that the way we store it is secure. As an institution of higher education, we are in the business of creating and teaching information, making the information we possess one of our most important assets. It follows that one of the most important obligations we have as a higher education institution is to keep our information, our data, secure. Additionally, SUNY, as a public institution of higher education, is subject to so many laws surrounding our information (NYS Breach Notification, FERPA, HIPAA, etc.), so it is crucial that any agreement for these services is codified into written terms, where we hold the vendor accountable for the same legal obligations that we as a higher education institution must comply with.

While it may be tempting to just put a service in place without having to work out terms, there is a general anecdote in the data privacy world: The cheaper and easier the service is to buy, the bigger problems it could potentially cause in the long term. If we purchase a cheap service to host our data, our most precious commodity, then we put our institution at risk, especially if we have failed to codify any standards with which our data must be protected. Given that information is our most important commodity, and given that we have additional obligations placed upon us by State and Federal law to keep our data safe, it is imperative that anyone who we give our data to should be held to minimum standards about protection of our data, and what they can and can't do with it.

Takeaway:

If a service seems easy and cheap, that should signal a red flag that the service could pose a larger risk to the institution down the line. The best advice for cloud storage, or any IT service where our information is involved, is to have any contract for such a service reviewed by counsel to make sure it has the necessary provisions and covers the necessary bases to hold our vendor to at least the same protections and standards that is expected of our institution.

Cloud Best Practices

In addition to ensuring that you codify the necessary contract terms with a vendor in a contract or less formal written agreement, you should also follow these best practices to ensure the safety of your data when you use the cloud:

1. **Ensure you have permission from the institution before using the cloud technology.**

   In other words, only use organization-approved cloud vendors, and do not sign up for any new technology service, and especially a cloud-based service, without permission. The institution will want to sign off on whether or not they will allow you to use the cloud storage system to house institutional data. Users need to be reminded that the information they possess is not their information, but the institution's information, so the institution has the ultimate say on which cloud vendors and storage solutions it deems appropriate for use.

2. **Know what information can and cannot be stored to the cloud.**

   Certain data may be so sensitive that your institution has decided it is not appropriate to store in the cloud hosted by a third party, regardless of the other safeguards you have put in place to ensure you retain control of the data and that the vendor has agreed to maintain the safety of the data. Therefore, make sure your institution determines what information should never be placed in the cloud, and then communicate that to employees for awareness, through your general security awareness training, when your institution has established their access to the cloud, by way of a disclaimer when they sign into the cloud service, or all of the above.

3. **Make sure that data, and especially data with heightened privacy interests, does not remain in the possession of a cloud service provider, and the information you upload is not utilized by the vendor for their own purposes.**

   Your institution wants to maintain control of your data at all times. At no point should the vendor who hosts the cloud service provider be able to access and use your data for their own purposes. As such, you want to be sure that the information that is shared with a third party cloud service provider is not retained by that vendor after the use of the provider ceases, and also that the information uploaded to the cloud is not used and retained by the cloud service provider themselves for their own purposes. A good example to illustrate this issue is a cloud service provider that checks for plagiarism by comparing student papers to previously written papers and works. Services like this may want to store your students papers into their database so that they can build upon the papers they have to check against. However, you would not want to have the vendor keep these student papers because they are the institutions education records that we have a duty to protect, and we should not allow them to be in the possession of a third party for the third party's use for their own purposes.

4. **Ensure work-related data is never copied or stored on personal cloud storage systems.**

   The personal cloud system you utilize for file sharing, file storage, music playback, or any other purposes does not have security protocols that have been vetted and approved by your campus institution. Therefore, you should never think it is okay to use your personal cloud services to store your work information.

5. **Use a Unique Password for Cloud Service Providers or Personal Accounts.**

   You should always use unique passwords to reduce the risk of potential loss that could result if a password is shared, stolen, or breached. This is a best practice for information systems that transcends cloud storage systems. You should also never use a password for a work or cloud storage system that you use for personal use. Your security measures for personal devices and systems are likely not as advanced as those of your institution.

6. **Ensure that Access on Cloud Service Providers is Restricted and that processes in place ensure that those who should no longer have access to information have their access privileges restricted.**

   Cloud Service accounts should be configured to restrict access to the information. In other words, everyone that can access the cloud account of the institution should not then have unfettered access to all the information posted to the cloud. Instead, access to information should be done by active, purposeful action to grant that cloud user access to a specific document or file.

   Therefore, the default access setup for your cloud service provider should be that access to information is restricted for everyone, and then an administrator can grant individual permissions to access information and files when necessary and appropriate.

   Since an institution should have a process for granting access, they should also have a process for removing or restricting access when someone should no longer have access to files or information. For instance, if a person moves from one area of the institution to another, they should not still have access to the cloud service provider containing information from the department they are no longer a member of. Similarly, if they leave the institution, access should be cut off immediately.

7. **Be sure you are running up to date antivirus software and that files are scanned prior to being opened.**

   Making sure that your computer is updated with the latest virus-scanning programs and software will better protect the institution if a compromised document is downloaded from the cloud to the institutions systems. Having updated anti-virus software is important, but it is especially critical when the institution is having data hosted on a third party cloud service provider that is not in their direct control. Although the Cloud Service provider must agree to adequate security safeguards before you agree to utilize them for your data, it is still important to secure at the institutional level because the third party vendor could breach their contract terms to keep their environment secure, or they could have been compromised in spite of their adequate security protocols.

What Do Written Terms for Cloud Services Try To Control

When we create a written agreement with a Cloud Service provider, we are attempting to codify certain elements that help us to ensure the privacy and security of our data.

Elements and considerations for cloud services:

The following are some elements and considerations for the arrangements of cloud services, and the terms that should be contemplated and codified between the institution and a cloud service provider prior to any information sharing.

1. Transparency:

Who has access to systems and data, and when and where they have access. The agreement should delineate the data, its locations, and access in detail. The clearer the terms with respect to these issues, the more able we are to retain some level of control over our data, even though it is in the hands of a third party.

2. Control:

Setting parameters for who should be allowed to have access to systems and data; and where data can (and cannot) be processed and stored. Specifically, the institution should know where the cloud service provider intends to physically store the data, because the data can be "in the cloud" but the reality is that the cloud has to be pointing to some physical location on land where the data resides. As a best practice, it is always better to require that the data stay in the parameters of the United States, because when a breach occurs, the laws that will become applicable based on the United States jurisdiction will be much clearer, and also because attempting to investigate any breach that involves servers and physical locations on another continent can and will exponentially increase the complexity and costs of managing the events that follow the breach.

One of the main roles of a Chief Information Security Officer at a higher education institution is to know what data you have, and where you have it. The CIO should perform the same due diligence to determine where the data will be hosted when dealing with a cloud service provider. Additionally, there are many regulatory considerations that would prohibit institution information crossing certain borders as a result of the type of information that is stored, and the sensitivity of the data. For example, some data cannot leave the United States, or may be classified as a "deemed export" that is prohibited from being accessed by foreign nationals under United States export laws. Violation of this law may jeopardize continued research funding for the institution and also potential criminal charges.

3. Ownership - Clouds vs. Their Contents

We need to make sure you make it clear who owns the data. Cloud service providers do not own the underlying software, but it should be made clear that the data we store on the cloud is SUNY's data. Institutions need to maintain ownership over raw data, but also the results of the data that may result from processing information on the cloud server.

4. Monitoring:

Being able to access information on data access to ensure that the actual access meets the terms of the agreement – that only those with authorization are accessing the data, and that those who are not authorized do not have access.

5. Security Protocols:

What security protocols must the cloud service host have in place before they can be entrusted with an institutions data. The institution can ask for the cloud service provider to agree to very specific security measures and industry standards, rather than a vague and general statement about keeping the data safe. In fact, the more specificity the contract has with regard to security protocols, the more likely the institution will be able to successfully hold the cloud service provider accountable in the event of a breach. That is, if the terms of security are left vague and open-ended, the cloud service provider will be able to say that they believe their security standards met the contract terms. However, if the contract specifies actions and protocols for security, and the cloud service provider deviated from those protocols, the institution will be in a better position when determining any culpability for the breach, and liability that flows from it.

6. Service Levels:

Typical cloud agreements define service level agreements (SLAs), which are parameters that establish providers' expected uptime and performance. The terms should help to establish expectations for the end-user experience and the customer service level that the institution should expect from the cloud provider. Service levels become especially important in times of emergency response or data recovery. Therefore, terms should be set that clarify expectations for service from the provider, especially in situations where recovery of the data is critical to the business operation of the institution, such as in times of crisis or natural disaster.

7. Legal Obligations:

Ensuring that the cloud service host will meet the same legal obligations that the institution is subject to, or at least aid in helping the institution meet its legal obligations by providing information the institution needs to comply with the various laws. These terms would include things like immediate notification by the host to the institution in the event of a breach, with information including what data was accessed, by whom, and how it was accessed.

8. Liability:

Identifying terms for who would be liable in the event of a breach. The cloud service provider should be held liable for any breach that arises when they are entrusted with hosting an institutions data. The logic here is that when we give another party our data and they breach it, they must be responsible. A good analogy to illustrate this concept uses an egg, where the egg

is an institutions data; when a cloud service provider is holding our eggs, they should agree to keep our eggs safe, and they should be liable for any damage to the egg that occurs when they had the egg. Simply stated, if an institution is paying a cloud host to hold its eggs, and the cloud host drops the egg, they owe the institution an egg – or the cost of the damages that resulted from the egg being damaged.

Terms codifying this liability should be included in written terms between the institution and the cloud service provider, where the cloud service agrees to be responsible for the privacy and safety of our data, and so when that data is breached, the cloud service provider agrees to be held responsible for the associated costs of the breach.

Institutions should not just think about actual damage (replacing the egg) but all the costs that flow from the breach, which can include:

- Legal fees
- Immediate cleanup costs and Incident Response
  - Forensics firm
  - Breach Notification
    - Identifying population that was impacted and their contact information
    - Notifying customers (where notification costs can be significant)
    - Call Centers
  - Fraud Prevention Measures
  - Setting up call centers and paying for free credit monitoring
  - Cost of hiring a crisis management firm
- Reputational damage that occurred as a result of the breach (often difficult to quantify)

The breach responsibility clause should be carved out specifically so that there is no ambiguity. The Cloud Service Provider will likely try to negotiate limiting language on breach responsibility (such as negotiating that they would "agree to cover the costs of a breach only upon proof that its action caused the breach." These are things that the Cloud Service Provider will try to negotiate, which is another reason why involving Counsel is the best practice.

With respect to notification, even if the vendor takes responsibility for making required notifications, the institution should have a strong role in drafting the language of the notification, and specifically including language regarding the culpability of the breach to protect the institution's reputation. Therefore, institutions should try to include terms that allow the institution, in the event of a breach, to identify the Cloud Service Provider by name in the breach notification that is sent to the individuals whose information was breached.

Campuses, and their campus counsel, should also be on the lookout for other language in the contract that limits overall liability, where their exposure would be limited to one or two times the cost of the contract. This type of a limitation should also be avoided, since the costs that flow from a breach can quickly add up. Industry estimates vary as to how much a breach can cost, but some estimates say a breach can cost $400 per record breach, where it can cost up to $25 dollars

for each call at a breach notification call center, up to $3 dollars for a notification letter, $600 per hour in forensic costs, and up to $75 per person for credit monitoring.

If you are negotiating terms with a small vendor, it may be a good idea to require proof of insurance, or proof of adequate set-asides to cover breach costs as part of the negotiated terms for additional assurance that the Cloud Service Provider could handle the costs of a breach.

With the amount of liability terms institutions seek from cloud service providers, it is only natural for them to have their own desired terms. Usually, cloud service providers will want institutions to assume liability for copyright-infringement or other illegal material that institution employees and students will place on the cloud platform, or to agree to be liable if the cloud is used for some other prohibited activity.

9. Data Availability:

In addition to where data will be located, and how it will be secured, the terms of a cloud service agreement should specify the institutions expectation for access to the data, where authorized users are assured that they will have access to the data hosted on the cloud when they need it. This access is especially important in the cloud, where internet interruptions may lead to unexpected outages that prevent an institution from accessing its own data.

10. Portability:

Portability is the concept whereby data is transferable from cloud to cloud, from campus servers to the cloud, or from the cloud back to the campus. This is an important concept, because cloud vendors are more eager to help get campuses data to their cloud, but they are less eager to help extract the data back out of the cloud. Campuses should consider what the cloud storage service is providing – simple data storage will be easier to migrate, whereas web-based platforms or applications that are proprietary are less likely to have data transferred. With systems where your data would need to be converted to a transferable format prior to transferring, the cloud provider will be less inclined to help with this data transfer when you are trying to stop using their services. If this requirement was part of the contract terms, they would be more inclined to help with this. If the cloud service provider refuses to agree to this, you might want to consider the file formats you will be left with in the event that you decide to pull your data off of the cloud service provider.

Resources

- The Cloud Security Alliance's Guidance for Critical Areas of Focus in Cloud Computing is a good industry resource for CIO's considering cloud computing and legal considerations, because the guidance contemplates the complexities of multi-nation clouds.

Recommended language for Cloud Service Contracts:

Contract Language Distributed by SUNY CIO in June of 2015

Data Privacy

a. Selected Firm/Vendor/Vendor will use SUNY Data only for the purpose of fulfilling its duties under this Agreement and will not share such data with or disclose it to any third party without the prior written consent of the SUNY, except as required by this Agreement or as otherwise required by law.

b. Campus SUNY Data will not be stored outside the United States without prior written consent from the SUNY.

c. Selected Firm/Vendor/Vendor will provide access to SUNY Data only to its employees and subFirm/Vendor/Vendors who need to access the data to fulfill Selected Firm/Vendor/Vendor obligations under this Agreement.

d. Selected Firm/Vendor/Vendor will ensure that employees who perform work under this Agreement have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of this Agreement.

e. If Selected Firm/Vendor/Vendor will have access to the SUNY's Education records as defined under the Family Educational Rights and Privacy Act (FERPA), the Selected Firm/Vendor/Vendor acknowledges that for the purposes of this Agreement it will be designated as a "school official" with "legitimate educational interests" in the SUNY Education records, as those terms have been defined under FERPA and its implementing regulations, and the Selected Firm/Vendor/Vendor agrees to abide by the limitations and requirements imposed on school officials. Selected Firm/Vendor/Vendor will use the Education records only for the purpose of fulfilling its duties under this Agreement for SUNY's and its End User's benefit, and will not share such data with or disclose it to any third party except as provided for in this Agreement, required by law, or authorized in writing by the SUNY.

If Selected Firm/Vendor/Vendor will receive, maintain, process or otherwise will have access to confidential information on employees of the Campuses of the State SUNY, it shall pursuant to the Gramm-Leach-Bliley Act (P.L. 106-102) and the Federal Trade Commission's Safeguards Rule (16 CFR Part 314), and to the extent the Firm/Vendor is a covered entity or applicable service provider under these regulations with respect to student or customer data, the Firm/Vendor will implement and maintain a written Information Security Program ("Program") in order to protect such confidential customer information. Customer information is defined as "any record containing nonpublic personal information as defined in 16 CFR §313(n)" (the FTC's Privacy Rule) "about a customer of a financial institution, whether in paper, electronic, or other form" (16 CFR §314.2). Examples of nonpublic personal customer information include, but are not limited to, name, address, phone number, social security number, bank and credit card account numbers and student identification numbers.

Data Security

In addition to the Data breach notification requirements provided in the solicitation document, the Firm/Vendor/Vendor agrees at all times to maintain network security which at a minimum, includes: network firewall provisioning, intrusion detection, and regular (three or more annually) third party vulnerability assessments, and share assessment results with SUNY. Further, the Firm/Vendor/Vendor agrees to maintain network security that conforms to generally recognized "Industry Standards "and best practices that the Firm/Vendor/Vendor applies to its own network. Generally recognized industry standards include but are not limited to the current standards and benchmarks set forth and maintained by the Center for Internet Security (see http://www.cisecurity.org) or Payment Card Industry/Data Security Standards (PCI/DSS) - see http://www.pcisecuritystandards.org/ .

New York Information Breach and Notification Requirements

The Firm/Vendor/Vendor hereby acknowledges and agrees to use commercially reasonable efforts to maintain the security of private information (as defined in the New York State Information Security Breach and Notification Act, as amended "ISBNA"(General Business Law § 889-aa; State Technology Law § 208) that it creates, receives, maintains or transmits on behalf of SUNY and to prevent unauthorized use and/or disclosure of that private information; and implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic private information that it creates, receives, maintains or transmits on behalf of SUNY("SUNY Data"). The Firm/Vendor/Vendor hereby acknowledges and agrees to fully disclose to SUNY pursuant to the ISBNA, and any other applicable law any breach of the security of a system where the Firm/Vendor/Vendor creates, receives, maintains or transmits private information on behalf of SUNY following discovery or notification of the breach in the system as to any resident of New York State whose private information was, or is reasonably believed to have been acquired by a person without valid authorization ("Security Incidents"). The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. The Firm/Vendor/Vendor shall be liable for the costs associated with such breach if caused by the Firm/Vendor/Vendor's negligent or willful acts or omissions, or the negligent or willful acts or omissions of the Firm/Vendor/Vendor's agents, officers, employees or subFirm/Vendor/Vendors. In the event of a Security Incident involving SUNY Data pursuant to the ISBNA, SUNY has an obligation to notify every individual whose private information has been or may have been compromised. In such an instance, the Firm/Vendor/Vendor agrees that SUNY will determine the manner in which such notification will be provided to the individuals involved pursuant to the ISBNA and agrees to indemnify SUNY against any cost of providing any such legally required notice. Upon termination or expiration of this Agreement, the Firm/Vendor/Vendor will follow SUNY's instructions relating to any SUNY Data remaining in the Firm/Vendor/Vendor's possession. Upon authorization from SUNY, the Firm/Vendor/Vendor will use data and document disposal practices that are reasonable and appropriate to prevent unauthorized access to or use of SUNY Data and will render the information so that it cannot be read or reconstructed.

Service Levels

SUNY understands that the Services will not be uninterrupted or error free. The Firm/Vendor/Vendor will use commercially reasonably efforts to ensure availability of the Services in accordance with the provisions of the "Service Level" Addendum annexed herewith as Attachment 1.

SERVICE LEVEL AGREEMENT (ATTACHMENT 1)

This Service Level Agreement ("**SLA**") sets forth the service level and performance objectives of the Firm/Vendor/Vendor in providing hosting services (the "**Services**") to SUNY. The Firm/Vendor/Vendor will use commercially reasonable efforts to meet the following service level and performance objectives to support the operation of the facilities, server(s), computer equipment, operating software and connectivity used to provide the Services to SUNY.

1. Uptime Commitment

The Firm/Vendor/Vendor will use commercially reasonable efforts to ensure the Firm/Vendor/Vendor's Systems are available 99.9% of the time (the "**Uptime Commitment**"). All Uptime Commitment will be measured within the Firm/Vendor/Vendor's System on a monthly basis calculated to include twenty-four (24) hours per day over each month, but excluding from the numerator and denominator in the calculation the duration in time of any temporary shutdowns due to scheduled maintenance (which will not exceed in the aggregate sixteen (16) hours per month), telecommunications or power disruptions caused by third parties, and any other causes beyond Firm/Vendor/Vendor's reasonable control. The Firm/Vendor/Vendor agrees to notify the Group promptly of any factor, occurrence, or event coming to its attention that may affect the Firm/Vendor/Vendor's ability to meet the Uptime Commitment, or that is likely to cause any material interruption in the Services.

2. Exclusive Remedy.

The Firm/Vendor/Vendor will use commercially reasonable efforts to correct any material problems in the Services, including any failure to satisfy the Uptime Commitment. In the event that the Firm/Vendor/Vendor fails to satisfy the Uptime Commitment for a given month, the Group's sole and exclusive remedy will be to receive a service credit equal to the following percentage of the monthly fees for the Services for the stated uptime:

97% to 99.9%	15%
94% to 96.9%	25%
92% to 93.9%	50%
90% to 91.9	75%
Below 90%	100%

In no event will the service credit exceed the monthly fees paid by SUNY for the Services. SUNY acknowledges and agrees that if the remedies set forth in this section are applied, any failure of the Firm/Vendor/Vendor to meet the requirements in this SLA will not constitute a breach of the Agreement.

3. Monitoring. Firm/Vendor/Vendor will monitor and maintain Firm/Vendor/Vendor's Systems in working order each day (24 x 7). Firm/Vendor/Vendor will proactively manage and monitor all application server hardware devices and software to ensure optimal performance and

reliability as well as to detect abnormal events or exceeded utilization or performance thresholds. Firm/Vendor/Vendor will proactively monitor the status of the operating systems (e.g., CPU, disk I/O, memory, processes, etc.), critical application layer daemons and processes and trigger appropriate event notification alarms caused by errors, exceeded thresholds, etc.

3.1 Maintenance.
Firm/Vendor/Vendor will operate, monitor and administer all servers, applications and networks supporting the Services. In order to provide such coverage, Firm/Vendor/Vendor may utilize a mixture of on-site and on-call support staff, automated server monitoring and automated paging technology. Contactor's on-site coverage is during Firm/Vendor/Vendor's normal business hours, Monday through Friday, excluding holidays recognized by Firm/Vendor/Vendor.

3.2 Scheduled Outages.
Maintenance outages, if necessary, will be conducted at a time and in a manner to minimize adverse impacts on the Services. Maintenance outages will include, but are not limited to the installation of upgrades, service packs and routine server or application configuration changes. Other maintenance outages may be necessary from time to time.

3.3 Change Control.
Firm/Vendor/Vendor will install new equipment, software, releases, upgrades, fixes, patches and other items necessary to maintain Firm/Vendor/Vendor's Systems to industry standards. Firm/Vendor/Vendor will proactively gather information from appropriate server, peripheral, operating system or database vendors regarding upgrades, defect patches or fixes.

3.4 Notice. Firm/Vendor/Vendor will use commercially reasonable efforts to give the Group three (3) days notice prior to all non-routine management, maintenance, change control or other actions by Firm/Vendor/Vendor that may material impact the Service adversely.

SUNY CAMPUSES AND CLOUD STORAGE GUIDANCE