Procuring Cloud Services – Recommendations for SUNY Oswego

This document is intended to act as a whitepaper to assist departments in acquiring cloud-based services at SUNY Oswego. It can act as a starting point for discussions across the institution on best practices and implementation procedures of these services.

Cloud-based service is an IT term that refers to utilizing information technology systems and services that are not located on your campus. Examples of these are Google GMail on our campus. It is a method of offering services that is becoming more popular, and in many instances, is the only way that a service is offered.

Success of any IT service-based project will depend on departments implementing the project to work together. If you have questions on this document or acquiring services, you should contact Sean Moriarty, Chief Technology Officer at SUNY Oswego.

Cloud-based services

As IT software and services are becoming highly commoditized and offered in the cloud, it is important for SUNY institutions to ensure that the services they utilize are appropriate, not just for the individual or the department, but also for the University or College. To maximize value and minimize risk for these services, it is best that the following questions be asked:

- What data will this service use? Will Personally Identifiable Information (PII) or confidential information be shared with a vendor?
- Are there FERPA requirements that need to be considered to protect the shared data?
- Does the application meet accessibility requirements?
- Does the vendor have the appropriate security measures in place for the data being stored?
- Is there already an existing SUNY contract with this vendor? If not, does the contract need to be reviewed by the CTO office and/or SUNY legal? Should a SUNY wide contract be considered?
- Will authentication be required to utilize the service? If so, has a plan to integrate the application with the institution's identity management system been scheduled into the project timelines?
- Will a data exchange project be required to obtain the service? If required, has a project been scheduled to implement the exchange?
- Will the application need to be customized with logo and branding? Has the proper team been created to implement these aspects of the project?

Purchasing services that move College data off campus need to be carefully considered to ensure data remains secure for the institution. When IT software and services are acquired, it is important to have your IT and purchasing departments involved in procuring the service. They will be able to assist in determining data requirements, the level of security that is required by law and the contractual obligations and procedures that must be followed to procure that service.

They will also assist in arrangements to schedule and manage a project if an identity management integration, data exchange project or branding is required with the vendor.

Procurement

Any software or service purchase starts with requirements analysis and an examination of options. More and more, institutions are starting to utilize cloud-based services as an answer to completing work and delivering services. Involving Campus Technology Services early when purchasing these services offers many advantages, including usually completing the project quicker. When procuring off-campus services, the following questions and items should be considered:

- What is the usage scope of the purchase? Is it University-wide, departmental or individual? Having an understanding of the scope will assist in determining risk. But it is important to understand that even services with a small usage may put Personally Identifiable Information (PII), private and confidential data at risk.
- What are the service requirements and what is the appropriate Service Level Agreement? Is the service required 24x7x365 or does it have more limited requirements? Are the vendor's service offerings in line with what you are looking for and do they have a proven record of success?
- What data is going to be shared with the third party provider and what are the legal requirements of handling that data based on your institution's data classification? Understanding your institution's data classification procedures will enable you to determine the security and compliance requirements, based on the appropriate legislation and university policies (legislation examples include PCI, FERPA, HIPAA, SUNY and university policy). Regardless of the data being used, consideration will need to be given to:
    - Data transmission: How will data be transmitted between Oswego and the service provider? Is it secure?
    - Data collection and use: How will the provider collect and use data from the school and your students? Are there any restrictions that may apply to the provider's use of that data? If so, it is important the contract binds the service provider to those uses and restrictions.
    - Are you outsourcing services that are normally done at the college, requiring that data be stored at a third party site? If so, you have essentially deemed the vendor will be acting as a "school official" under FERPA. It is important to know that outsourcing services does not remove the institution from requirements to protect data.
    - How is the vendor going to handle your data? Is the vendor allowed to use your data and re-disclose to others? What if they are served with a subpoena? You should obtain assurances from the provider that the data will not be disclosed without written permission, including assurances that your vendor will provide your institution both the right to review any data prior to re-disclosure and to verify proper disclosure avoidance techniques have been used within reason.

- When the contract is complete and will not be renewed, what are the vendor's data retention and disposal procedures pertaining to the school and its students. It is important to know that all data disclosed to the provider or collected by the provider must be disposed of by secure means, to ensure that it is protected from unauthorized access or use.

When needs are being analyzed, it is a good time to look at project planning on implementation. Many institutions look at scheduling and resourcing implementation projects at this stage of the analysis:

- Does the service require authentication to access? If so, do they utilize authentication services that your institution supports? If so, can a timeline for implementation be planned and scheduled with IT for the appropriate period?
- Will the service require any institutional branding? If so, it is best to involve corresponding staff to analyze the time requirements and ensure they schedule this work into their timelines.
- Will the service require a data integration and exchange project? Will the vendor work with you to implement this or will it be a separate contract and engagement? At this stage, it is a good time to bring the appropriate staff in to analyze scope and scheduling.

The Contract

Once you have determined the requirements, it will be important to ensure the terms and agreements of the contract are met. Contracts can be tricky and extremely detailed. It is best to expect that the contract will need to be examined by legal counsel, but the purchasing department and CTS will be able to best determine the route your contract needs to take. Important considerations include:

- Have any other SUNY institutions procured this software and are there already any other SUNY contracts available to utilize?
- Make sure you have purpose, scope, duration and the data that is being disclosed spelled out in the contract.
- Identify all elements that comprise the agreement and in what order precedence will be followed in the event of a contradiction in terms. Identify any contract terms that are incorporated by reference to another contract.
- Depending on the required level of service, the contract should be clear on the service levels and support, and any credit you will receive for failure by the provider to meet the service levels.
  The contract should also require the provider to supply the institution with all the technical assistance required to setup and use the services
- Where will the governing law and jurisdiction of the contract be located? Typically, a provider's default contract will state that the law of the provider's home state governs.

Public institutions generally have significant restrictions on their ability to consent to such provisions under the school system's state laws. You may need to require that the governing law and jurisdiction be New York State.

- Identify all legal requirements that the contract will need to cover. It is important to remember that FERPA may not be the only law that governs your agreement. The agreement could broadly require compliance with all applicable federal, state and local laws and regulations, and identify those authorized (whether express or implied) to permit the audit, evaluation, enforcement or compliance activity.
- Identify in the contract where the data will be stored. Ideally the data will be stored in the US, but if it is not, the contract must ensure data be stored in countries that offer an international safe-harbor treaty. The jurisdiction of the contract should still be New York State, since a contract in a foreign country may present difficulties to ensure compliance in the case of a breach.
- It is important that the service you are acquiring comply with New York state accessibility laws. The vendor should be able to provide a VPAT (voluntary product accessibility template) and assurances the product meets NYS accessibility compliance.
- What is the duration of the contract? How will it be terminated? Does notice need to be given to terminate? Can the contract be modified during the life of the contract? Establish how long the agreement will be in force and what the procedures will be for modifying the terms of the agreement (mutual written consent to any changes is a best practice).
- What happens to data at the termination of the contract? What are both parties' responsibilities upon termination of the agreement—particularly regarding disposition of student information maintained by the provider? Upon termination of the contract, the provider should return all records or data and properly delete any copies still in its possession, including archives and/or backups.
- Moving data to a service provider does not release the institution of any of their responsibilities in the case of a data breach. For this reason, the service provider should be held liable for the activities of its staff and subcontractors to ensure institutional data is properly handled. Suggestions for ensuring data will be handled securely and that privacy is maintained include:
    - Require that any subcontracting, use of other providers, etc., only be allowed upon written approval by the school.
    - Specify what happens to your school's data if the provider goes out of business or is acquired by another firm. Is there a source code or data escrow provision?
    - Verify that your authorized representative has appropriate disciplinary policies for employees that violate data policies.
    - Verify that your authorized representative has a training program to teach its employees about protecting PII and data from education records.
    - Bind individuals to the agreement, including not only the vendor to whom you are disclosing PII from education records, but also the individuals who will be accessing that data. There are several ways to accomplish this. One way is to

identify the individuals in the agreement itself and have them execute the agreement in their individual capacity, as well as having a representative execute the agreement for the entity. Alternatively, your agreement can require individuals accessing the PII from education records to execute affidavits of nondisclosure or other documentation that indicate their individual agreement to handle the PII from education records properly.

- Your agreement should be clear about limitations on the use of PII from education records, specifically stating it can only be used for the activities described in the agreement. Your agreement may also address methodological limitations, for example, identifying which data sets, if any, to which the PII may be linked.
- The vendor should be able to verify SAS 16 auditing and to provide audit reports to you.
- You should set clear expectations so your authorized representative knows what process needs to be followed for the proper destruction of PII from education records.
- Require vendors to disclose any past data management or PII violations.
- Your written agreements should specify points of contact and data custodians (the individual(s) directly responsible for managing the data in question).

Conclusion

Moving IT services into the cloud is commonplace, and opportunities to utilize these services will only continue to increase. Ensuring Oswego has sound practices in acquiring these services, creating the legal agreements and secure data practices with the vendors that we partner with, will assist departments to become more effective and efficient as well as minimize risk and maximize value.

It is important to involve Campus Technology Services early when you are considering a cloud agreement. Negotiating these contracts can be time consuming and CTS will help ensure contracts are negotiated to minimize risk for the College and conform to Oswego, SUNY and New York state requirements. CTS will partner with you to help move the project from contract negotiations to implementation in a time appropriate manner.