



Requirements for Technology Outsourcing

Table of Contents

Revision History	3
Overview	4
Service Provider Selection	5
Service Delivery Models.....	5
Legal Considerations	5
Security Assessments.....	6
Data Protection & Transmission	6
User Access Control	6
Service Availability	7
Contractual Considerations	8
Due Diligence of the Contract.....	8
Contract Definitions	8
Data Handling.....	9
Data Compromise	10
Data Retention	10
Litigation Response	11
Data Security	11
Service Availability	12
Final Considerations.....	13

Revision History

Author	Date	Description
Kent King	18-Nov-2011	First review draft
Kent King	12-Dec-2011	Heavy revision of review draft
Kent King	20-Dec-2011	Final cleanup for first release

Overview

The exponential growth in cloud services presents many opportunities for Denison University to outsource some internal services. To look at an outsourcing opportunity solely as a financial proposition does not serve the University interests and will expose Denison to potential risks and liabilities. This document provides guidance for minimizing these risks and insuring that the true cost of outsourcing does not exceed the benefits of the service.

When considering an outsource service provider, many factors will contribute to the actual cost of the service. There are significant intangible costs; the greatest of these would be the reputation of Denison University. A data breach would be seen as a failure of the University even if the contract stipulated the financial responsibility of the service partner. For that reason, any plan to outsource sensitive data must be carefully reviewed and approved at an appropriate level for the commensurate risk.

The principles of cloud computing which make it very flexible and affordable create a relationship dynamic which must be mitigated by *ongoing* risk management. A portion of the cost savings obtained by cloud computing services must be invested into the increased scrutiny of the security capabilities of the provider and ongoing detailed audits to ensure requirements are continuously met. Throughout this document, the terms cloud provider and service provider will be used interchangeably to remind the reader that these services are external to the Denison University Information Technology Services.

This document is presented in three sections. [Service Provider Selection](#) will provide some “food for thought” when evaluating an outsource provider. This section will also define terminology and present broad risk issues present in any outsourced service. [Contractual Considerations](#) will outline items that should be included (or considered for inclusion) in the contract itself. Finally, for vendors that will handle personal or financial information, a formal questionnaire is provided as a separate document. This security evaluation is a “self-assessment” to be completed by the vendor. It is *required* for the chosen candidate, and can also be used to measure risks between final candidates during the selection process.

Service Provider Selection

Service Delivery Models

There are currently three predominate technology service delivery models. It is critical to be aware of the tradeoffs between extensibility (openness) and security responsibility within these three models when considering a service offering.

- Infrastructure as a Service (IaaS) - Greatest extensibility and least amount of security responsibility accepted by the service provider. Denison assumes the majority of the risk in protecting data and keeping the service available. Plan to deploy applications in a way that is abstracted from the system itself. Backups should also be machine independent.
- Platform as a Service (PaaS) - lies somewhere in the middle, with extensibility and security features which must be leveraged by Denison. Insure that application development techniques are followed to minimize potential lock-in. The onus is on the University to have portability as a key design goal and an architecture that supports the necessary abstraction layers to make this achievable.
- Software as a Service (SaaS) - least extensibility and greatest amount of security responsibility taken on by the service provider. To protect against a service failure, plan to perform regular data extractions and backups to a format that is usable and not proprietary to the SaaS provider.

Denison University must perform extensive due diligence of any cloud provider for use in mission critical business functions or for hosting any sensitive information. If the provider will have any access to personal or financial data on behalf of the University, they must complete the Denison Vendor Security Assessment *prior to the signing of a contract*. The Information Security Officer will review the vendor responses, assess the risks associated with personal or financial data, and provide guidance on the suitability of the vendor.

Legal Considerations

Outsourced services challenge the presumption that organizations have control over data for which they are legally responsible. Electronic discovery has become an essential function to which a service provider is indispensable; if neglected by Denison, the adverse legal risks are substantial.

A service provider is a custodian of primary data assets for which the University has legal responsibilities to preserve and make available in legal proceedings (electronic discovery). Denison must have a clear understanding of the circumstances under which our data assets could be seized by a third party or government entity. Finally, Denison University and the service provider must have a mutual understanding of each other's roles and responsibilities related to electronic discovery, including such activities as litigation hold, discovery searches, providing expert testimony, etc.

From a risk management perspective, unencrypted data existent in the cloud should be considered "public" by Denison University. If encryption is used to protect sensitive data, segregate the key management from the service provider hosting the data, creating a separation of responsibility. This

protects both the cloud provider and Denison University from conflict when being compelled to provide data due to a legal mandate and can potentially solve some problems in electronic discovery.

Security Assessments

Many providers today have already obtained and freely provide “standardized” external assessments. While SSAE-16 (formerly the SAS-70 Type II) and ISO 27001 attestations can indicate widely varying levels of security competency, in the aggregate they are better than no assessment whatsoever. It is critical to examine the scope of SSAE-16 and ISO 27001 reviews because *the provider defines the scope of such assessments*. If possible, obtain these documents from competing providers during the selection process to allow the Information Security Officer time to review and comment.

Data Protection & Transmission

The University must understand all data placed in the possession of the service provider. The department or organization considering outsourced services must classify data and systems to understand compliance requirements. Data transfers between the University and the service provider must be adequately protected. Web forms and reports are typically protected using HTTPS. If there will be data file transfers, other methods to secure the files may be required. Contact the Information Security Officer if your project has any concerns about data transfers to explore secure procedures and processes.

There are several voluntary compliance organizations which service providers may affiliate with to show a level of due diligence. These are commonly called trust seals, and may include names like TRUSTe, Trust-Guard, Verisign or Safe Harbor from the US Department of Commerce. Compliance with a trust seal does not provide complete assurance against a data breach; however it does indicate strong awareness regarding customer data sensitivity and data protection. All other considerations being equal, a site with a reputable trust seal is a preferred service provider.

Finally, should the unthinkable happen and the provider does suffer a data breach, when and how will Denison be notified of the event? What penalties will the service provider bear? These items are typically included in a service provider contract. Suggested wording and considerations are included in the next section. However, if the project will involve sensitive information, the contract should be reviewed by the University’s legal counsel.

User Access Control

Access control is a critical and often over-looked consideration for the cloud service provider. In the practical sense, access control is how the user gains access to the service. The most common method will be a username and password. Recent advances on the Internet have made “federated” identities possible and very desirable. A federated identity would allow a user to use their existing Denison ID and password to access a service. Denison can support the Central Authentication Service (CAS) model, which itself can interface with other federated authentication services. Technical information regarding federated authentication compatibility may be obtained from the Information Security Officer.

If a federated identity is not available or desirable, other considerations must be addressed. If sensitive data will be handled by the service provider, all of the following concerns must be addressed before the service can be implemented:

- Who will be responsible for creating accounts for new users?
- How are requests for new accounts validated?
- How are ID's and passwords maintained and updated?
- What are the password requirements?
- How will accounts be removed or discontinued for users that have any change in status? (NOTE: this is more than just removing an account upon termination: A job change which takes the person to a different department may require the removal of access to a critical service.)

As can be seen from the list of concerns for separate accounts, using a federated identity provides a more secure and better controlled environment with less overhead than separate accounts. When evaluating a service provider, please contact the Information Security Officer to discuss possible authentication models with the vendor(s) if possible.

Service Availability

An often overlooked factor impacting availability is the range of other clients that the provider sells service to and how they use it. This information can be difficult to obtain. As an example, suppose the provider is selling a textbook service. How well does their system work near the beginning of a semester when all of their clients are trying to obtain the same service? As part of the due diligence on a service provider, try to obtain information about how they handle peak loads, when they expect these loads and how long they can maintain a higher than average level of service.

One of the reasons that an outsourced service provider is attractive is the "high availability" aspect. Service providers will often speak of the uptime in terms of percentages such as "99.995% uptime", but you must closely examine their definition of uptime and exclusions to see if the service will really work for Denison. Shared services and virtualized systems have almost eliminated system downtime. However, network services, application availability and other factors can still cause downtime. In addition, the days of a "maintenance window" are waning; systems no longer need to go down for periodic maintenance as frequently. Look closely at the contract for penalties when availability times are not met. Additional contractual wording and recommendations are included in the next section.

Contractual Considerations

Contracts are a key legal enforcement mechanism and must be negotiable to reflect the University's unique needs and the dynamic nature of cloud computing. Contracts are not Denison's only governance tool but should encompass the broad due diligence required of a service provider. During contract negotiations, plan for both an expected and unexpected termination of the relationship and for an orderly return or secure disposal of University assets and information. Understand that there may be conflicts between the laws the service provider must comply with and those governing Denison University.

Negotiate penalties payable by the service provider for data breaches to ensure this is being taken seriously by the provider. If practical, Denison University should seek to recover all breach costs as part of their provider contract. If impractical, the University should explore other risk transference vehicles, such as insurance, to recover breach costs. Such additional costs may offset the financial viability of an outsourced service and should be considered before signing any contract.

Understand the cloud provider's key risk and performance indicators and how these can be monitored and measured from the University's perspective. Cloud services are still in their infancy and there are a significant number of failures, buyouts and takeovers occurring within the sector. Look closely at the financial viability of possible service providers and if they might be a buyout or takeover target. Know how the business will be impacted if the provider "vanished" suddenly and have a plan to deal with this possibility.

Due Diligence of the Contract

It is important to remember that contracts are changeable and negotiable until they are signed. Some providers may insist on using their contract as the basis for a services agreement. Denison University also has its own contract templates which may be used as well. However, due to the rapid changes in the service provider world, any contract being considered should be carefully examined and assessed. If the contract is provided by the cloud service, Denison legal counsel should review and approve the contract prior to signing.

When assessing and reviewing a cloud service contract, various issues should be clearly defined and understood in the document. The list of points which follows should be carefully reviewed. Not all the points noted may be applicable to a specific agreement. Some items may need to be changed to better describe the service requirements on behalf of the University. Each item here is composed of a possible proposed contract wording and a rationale for including this in the contract.

Contract Definitions

Rationale: Closely examine the definition of terms in the contract to insure that Denison data is adequately defined and protected in the contract.

"Data" means information whether in oral or written (including electronic) form, created, obtained, transmitted, used, maintained, processed, and disposed of by Customer, End Users, and Vendor in the

course of using and configuring/providing, respectively, the Services under this Agreement, and includes Customer Data, End User Data, and Personal Data.

“Data Compromise” means a security-relevant event in which the security policy of a system used to create, transmit, maintain, use, process, or store data is disobeyed or otherwise breached, and in which Data is exposed to unauthorized disclosure, access, alteration, or use.

“Personal Data” includes but is not limited to: personal identifiers such as name, address, phone number, date of birth, Social Security Number, and student or personnel identification number; Protected Health Information (PHI) as that term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; personally identifiable information contained in student education records as that term is defined in the Family Educational Rights and Privacy Act, 20 USC 1232g; non-public personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; other financial account numbers and/or access codes; driver’s license number; and other state- or federal-identification numbers such as passport, visa or state identity card numbers [add here any Denison or state-law specific additions to the notion of “personal” data].

Data Handling

Rationale: Clearly define the Denison University requirements regarding data mining and access to data by the provider’s employees and partners.

Vendor will use Customer Data and End User Data only for the purpose of fulfilling its duties under this Agreement and for Customer’s and its End User’s sole benefit, and will not share such data with or disclose it to any third party without the prior written consent of Customer or as otherwise required by law. By way of illustration and not of limitation, Vendor will not use such data for Vendor’s own benefit and, in particular, will not engage in “data mining” of Customer or End User Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by Customer. [Depending on nature of services and data at issue] [Optional: All Customer and End User Data will be stored on servers, located solely within the Continental United States.]

Vendor will provide access to Customer and End User Data only those Vendor employees and subcontractors who need to access the data to fulfill Vendor’s obligations under this Agreement. 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, and have undergone all background screening and possess all qualifications required by Customer [alternative: “undergone all background screening and possess all qualifications appropriate to the nature of the employees’ duties and the sensitivity of the data they will be handling,”] prior to being granted access to the Data.

Data Compromise

Rationale: All provider contracts must include language to explicitly notify Denison of a breach event. Financial obligations of the event must also be clearly and carefully documented. The contract should be reviewed to insure there is no conflict with the section regarding [Ligation Response](#).

Immediately upon becoming aware of a Data Compromise, or of circumstances that could have resulted in unauthorized access to or disclosure or use of Customer or End User Data, Vendor will notify Customer, fully investigate the incident, and cooperate fully with Customer's investigation of and response to the incident. Except as otherwise required by law, Vendor will not provide notice of the incident directly to the persons whose data were involved, CSG-NACUA Shared Services Working Group – Model Contract July, 2010 regulatory agencies, or other entities, without prior written permission from Customer.

Notwithstanding any other provision of this agreement, and in addition to any other remedies available to Customer under law or equity, Vendor will reimburse Customer in full for all costs incurred by Customer in investigation and remediation of such Data Compromise, including but not limited to providing notification to third parties whose data were compromised and to regulatory agencies or other entities as required by law or contract; the offering of [X] months' credit monitoring to each person whose data were compromised; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Data Compromise. [alternative – add at end, "unless the Data Compromise was not due to negligence or misconduct on the part of the Vendor, in which case Vendor and Customer shall share the above costs equally"]

Data Retention

Rationale: Define the requirements for ongoing storage, retention and finally data destruction of Denison University data. The return of data at the termination of the Agreement should also be included.

Vendor will use commercially reasonable efforts to retain data in an End User's account, including attachments, until the End User deletes them or for an alternative time period mutually agreed by the parties. Using appropriate and reliable storage media, Vendor will regularly back up Customer and End User Data and retain such backup copies for a minimum of [Denison defined timeframe]. At the end of that time period and at Customer's election, Vendor will either securely destroy or transmit to Customer repository the backup copies.

Upon Customer's request, Vendor will supply Customer a certificate indicating the records destroyed, the date destroyed, and the method of destruction used. Vendor will retain logs associated with End User activity for a minimum of [x period of time], unless the parties mutually agree to a different period.

Upon termination or expiration of this Agreement, Vendor will ensure that all Customer and End User Data are transferred to Customer or a third party designated by Customer securely, within a reasonable

period of time, and without significant interruption in service, all as further specified in the Technical Specifications attached as Exhibit ____.

Vendor will ensure that such migration uses facilities and methods are compatible with the relevant systems of the transferee, and to the extent technologically feasible, that Customer will have reasonable access to Customer and End User Data during the transition.

Litigation Response

Rationale: Be sure the contract clearly defines the roles and responsibilities of both the vendor and Denison University in the event of a data discovery request.

Response to Legal Orders, Demands or Requests for Data except as otherwise expressly prohibited by law, Vendor will: (i) immediately notify Customer of any subpoenas, warrants, or other legal orders, demands or requests received by Vendor seeking Customer and/or End User Data; (ii) consult with Customer regarding its response; (iii) cooperate with Customer's reasonable requests in connection with efforts by Customer to intervene and quash or modify the legal order, demand or request; and (iv) upon Customer's request, provide Customer with a copy of its response.

If Customer receives a subpoena, warrant, or other legal order, demand or request seeking Customer or End User Data maintained by Vendor, Customer will promptly provide a copy to Vendor. Vendor will promptly supply Customer with copies of data required for Customer to respond, and will cooperate with Customer's reasonable requests in connection with its response.

Vendor will immediately place a "hold" on the destruction under its usual records retention policies of records that include Customer and End User Data, in response to an oral or written request from Customer indicating that those records may be relevant to litigation that Customer reasonably anticipates. Oral requests by Customer for a hold on record destruction will be reduced to writing and supplied to Vendor for its records as soon as reasonably practicable under the circumstances. Customer will promptly coordinate with Vendor regarding the preservation and disposition of these records. Vendor shall continue to preserve the records until further notice by Customer.

Data Security

Rationale: Review any vendor-provided wording regarding data security. Projects involving sensitive data should include a requirement for the vendor to complete the Denison Vendor Security Assessment.

Vendor will use industry-standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services under this Agreement. All facilities used to store and process Customer and End User data will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Vendor's own data of a similar type, and in no event less than reasonable in view of the type and nature

of the data involved. Without limiting the foregoing, Vendor warrants that all Customer Data and End User Data will be encrypted in transmission (including via web interface) at no less than 128-bit level encryption [or cite NIST, ISO, or FIPS standards], and that Vendor will comply with all other technical specifications of Customer provided in Exhibit ___. [Technical specs are where any other standards or requirements Denison wishes to include in the agreement, e.g. HIPAA security standards]

Service Availability

Rationale: Be sure that the contract clearly enforces the availability requirements of the project. Define penalties for the vendor when availability requirements are not met.

Vendor warrants that the Services will be performed in a professional and workmanlike manner consistent with industry standards reasonably applicable to such Services. Vendor further warrants that the Services will be Operational at least 99.99% of the time in any given month during the term of this Agreement, meaning that the outage or downtime percentage will be not more than .01%. [Alternative: or other standard as stipulated in RFP response and agreed to by the parties] In the event of a Service outage, Vendor will (a) promptly and at Vendor's expense use commercial best efforts to restore the Services as soon as possible, and (b) unless the outage was caused by a Force Majeure event, refund or credit Customer, at Customer's election, the pro-rated amount of fees corresponding to the time Services were unavailable. Neither party will be liable to the other for any failure nor delay in performance under this Agreement to the extent said failures or delays are proximately caused by forces beyond that party's reasonable control, provided that the party resumes performance as soon as it is reasonably able to do so.

From time to time it may be necessary or desirable for either the Customer or Vendor to propose changes in the Services provided. Such changes shall be made pursuant to the Change Control Procedure attached as Exhibit ___. [It is contemplated that this exhibit would indicate the different levels of change, and the corresponding level of authorization needed, including the ability for Vendor to make nonmaterial changes without Customer authorization] Automatic upgrades to any software used by Vendor to provide the Services that simply improve the speed, efficiency, reliability, or availability of existing Services and do not alter or add functionality, are not considered "changes to the Services" and such upgrades will be implemented by Vendor on a schedule no less favorable than provided by Vendor to any other customer receiving comparable levels of Services.

Final Considerations

When considering any outsourced technology service, we encourage you to contact the Chief Information Technology Officer or the Information Security Officer. They will be able to advise and engage the appropriate ITS staff and resources in the process. The earlier the inclusion, the smoother the process becomes: It is far easier to include requirements up front in the RFP than it will be to try to request a contract change after it has been signed! ITS can work with any campus department or organization to assist in this process and help protect University assets and our reputation.

For additional information and further guidance, please contact the Denison University Information Security Officer at ITSecurity@denison.edu.