Software as a Service (SaaS) Risk Policy

Policy

All Software as a Service (SaaS) applications or products proposed for integration with College systems and for the use of the College community must be reviewed to ascertain compatibility with College systems and to ensure that the College does not face unreasonable risks using the product. IS will work with the originating department to conduct a risk assessment before a purchase or utilization decision can be finalized.

I. DEFINITIONS

Software as a service (**SaaS**, typically pronounced 'sass') is a software delivery model in which a software application is developed and hosted by an application service provider (ASP) and customers access the application over the Internet. The SaaS vendor owns the software, runs it on computers in its data center and provides all support to the customers. The customer does not own the software but effectively rents it, usually for a monthly or annual fee. SaaS is not the same as the hosted software delivery model where the customer buys the software and places it within a vendor's facility.

A **Service Level Agreement** (SLA) is a negotiated agreement between two parties where one is the customer and the other is the service provider. In the situation of a SaaS arrangement this should be a legally binding formal contract. The SLA records a common understanding about services, risk mitigation, priorities, responsibilities, guarantees, and warranties. Each area of service scope should have the "level of service" defined. The SLA may specify the levels of availability, serviceability, performance, operation, or other attributes of the service, such as billing.

A risk analysis of a SaaS initiative should consider five **security objectives**; Confidentiality, Integrity, Use Control, Availability and Accountability. There is no standard for acceptable risk, each department will have different requirements and different tolerances for failing to meet a requirement. Therefore the department needs to conduct a risk assessment before a purchase decision is made.

Confidentiality is the security objective to prevent disclosure of inappropriate information; for example personal and private information or credit card information.[a]

Integrity is the security objective to prevent unauthorized or inappropriate changes and ensure that information maintains internal and external consistency.[b]

Use Control is a security objective considering a user's ability to perform actions on information such as download, copy or distribute sensitive information that is stored or used by an application. It can be malicious intent or a simple mistake that causes the release of sensitive information. [c]

Availability is a security objective to make sure particular information is available and useable for its' intended purpose when it is needed.

---

[a] Eric Maiwald. "Consideration for Risk Management When Choosing Software as a Service." Burton Group. 29 Jan 2008.
[b] Maiwald, pg. 9.
[c] Maiwald, pg. 11.

Accountability is the security objective that requires individuals be held accountable or held answerable for actions. It includes the ability to identify and authenticate users and audit trails to record actions.

II. OVERVIEW

SaaS is most appropriate for areas where the business processes are standardized, the data is not overly sensitive and the internal infrastructure requirements are substantial. SaaS applications can be configured for the college's needs but generally cannot be customized. With SaaS, business processes are treated as a commodity to achieve operational efficiency rather than a customized process that provides a competitive advantage.

III. RISK ANALYSIS

The purpose of this policy is to provide basic guidelines of security considerations for Data Stewards[a] when a Connecticut College organization is evaluating a SaaS offering. A full risk assessment should be conducted before a final purchase decision is made. A Service Level Agreement should be executed to outline the responsibilities and risk assumptions of the service provider and those of the college.

Please consider the following as you review Software as a Service offerings. Use the letters in parenthesis as a guide: The higher your (A)vailability, (I)ntegrity or (C)onfidentiality requirements are, the more critical the responses to these questions become.

Functionality

_____ Does the SaaS offering of the application have all of the features of the on-site, internally installed offering of the same product?

_____ If not, are there any critical features absent from either choice?

_____ Is the ASP aware of legal discovery and retention requirements and will they comply with a litigation hold request?

Availability

_____ What Service Level Agreement options are available from the SaaS offering?

_____ Does the contract contain penalty clauses for SLA nonconformance?

_____ Will the company provide metrics regarding conformance of SLAs with other clients?

_____ Do the terms of the Service Level Agreement meet your business needs?

Integration

_____ Will the SaaS offering of the product require integration with any existing, internal, College applications/systems?

_____ If so, what are the patching and upgrade coordination plans?

_____ What are the network and network security requirements for such integration?

Change Management

_____ Are patches, service level releases and other upgrades handled consistent with expectations?

_____ Are changes to the SaaS offering's environment conducted in a replica test environment before they are promoted to production?

_____ Who approves such promotions? Is it approved by our organization?

_____ Will we as an organization be involved in any development and testing?

Data Access

_____ How will the SaaS offering use our organization's data? Will the company use our information only as we intend them to?

_____ Will we receive a copy of the SaaS offering's privacy policy? Is the privacy policy consistent with how we expect them to utilize the information?

_____ Will the SaaS offering allow our organization to import and export data to and from the SaaS solution?

_____ Will we have full access to all of our data at all times within the SaaS offering?

_____ Is our data completely segregated from any other clients of the SaaS offering?

_____ If our organization terminates the agreement with the SaaS offering, what happens to our data?

Data Security/Use Control

_____ What are the SaaS offering's stated theft-prevention mechanisms?

_____ Will our organization be notified in the event of a data breach? How will we be notified? Is the notification timely and contractually required?

_____ Does the vendor conduct third party penetration and application security tests on a regular basis?

_____ Will we receive third party penetration and application security test results?

_____ Will the company offer legal commitments with regards to their security measures?

_____ Does the SaaS offering's security controls meet all of our organization's regulatory compliance requirements?

_____ Has the vendor conducted a Statement on Auditing Standards (SAS70) or other third party audit?

_____ Will the vendor share the SAS70 results?

_____ Has the vendor had any breaches within the last two years?

_____ Does the vendor host any data outside of the USA? Do the countries where the data is hosted provide sufficient legal protections to ensure the confidentiality of our information?

Human Resources

_____ Are all employees of the SaaS offering's company required to sign non-disclosure and confidentiality agreements?

_____ Are the employee screening policies and procedures satisfactory? (Do they conduct background or credit checks?)

_____ Are employee accounts reviewed periodically for appropriate access?

_____ If the SaaS offering's company outsources any job functions, what are the non-disclosure and confidentiality agreements, and employee screening requirements of the out-sourced agencies?

_____ Does the vendor outsource any job functions outside of the USA? Do the countries where job functions are outsourced provide sufficient legal protections to ensure the confidentiality of our information?

Physical Security

_____ Are the SaaS offering's data center(s) access controlled sufficiently?

_____ Are appropriate environmental controls in place in the SaaS offering's data center(s)?

Business Continuity and Disaster Recovery

_____ How frequently is the SaaS offering's system/application backed up?

_____ How frequently is our data backed up by the SaaS offering?

_____ Are those backups encrypted?

_____ Are those backups tested?

_____ Are those backups performed or transported off-site?

_____ Will our organization have the ability to perform our own backups of our data from the SaaS offering?

_____ How quickly can the SaaS offering recover from a catastrophic failure?

_____ How often are the business continuity and disaster recovery plans tested and reviewed?

[a] Data Steward is an individual who is responsible for business processes within their areas of supervision and protecting confidentiality and integrity of electronic and paper data maintained in their area.