	Guidelines: Software as a Service (SaaS) Security Guideline	No. 2010-1	Rev. 01-25-2010
		Date Approved:	2/10/2010
		Authors:	Bret Ellis/Jean Fruth
		Filename:	Software as a Service

I. DEFINITIONS

Software as a service (**SaaS**, typically pronounced 'sass') is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. The SaaS vendor owns the software and runs it on computers in its data center. The customer does not own the software but effectively rents it, usually for a monthly fee. SaaS is sometimes also known as hosted software.

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 an SaaS arrangement this should be a legally binding formal contract. The SLA records a common understanding about services, 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.

II. PROCEDURE

The purpose of this document is to provide basic guidelines of security considerations for Data Stewards when a Weber State University 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 university.

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 or (C)onfidentiality requirements are, the more critical the responses to these questions become.

Functionality

_______ Does the SaaS offering of the product 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 vendor aware of legal discovery and retention requirements and will they comply with a litigation hold request?

Reliability

_______ (A) What Service Level Agreement options are available from the SaaS offering?

_______ (A) Does the contract contain penalty clauses for SLA nonconformance?

_______(A) Will the company provide metrics regarding conformance of SLAs with other clients?

_______ (A) 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, on-site applications/systems?

_______(A) If so, what are the patching and upgrade coordination plans?

_______ (C,A) What are the network and network security requirements for such integration?

Change Management

_______(C,A) Are patches, service level releases and other upgrades handled consistent with expectations?

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

_______ (A) Who approves such promotions? Is it approved by our organization?

_______ (A) Will we as an organization be involved in any development and testing?

Data Access

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

_______(C) 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?

_______(C,A) Will the SaaS offering allow our organization to import and export data to and from the SaaS solution?

_______ (C) Will we have full access to all of our data at all times within the SaaS offering?

_______ (C) Is our data completely segregated from any other clients of the SaaS offering?

_______(C) If our organization terminates the agreement with the SaaS offering, what happens to our data?

Data Security

_______(C) What are the SaaS offering's stated theft-prevention mechanisms?

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

______(C) Does the vendor conduct third party penetration and application security tests on a regular basis?

______ (C) Will we receive third party penetration and application security test results?

______(C) Will the company offer legal commitments with regards to their security measures?

______(C) Does the SaaS offering's security controls meet all of our organization's regulatory compliance requirements?

______(C) Has the vendor conducted a SAS70 or other third party audit?

______ (C) Will the vendor share the SAS70 results?

______ (C) Has the vendor had any breaches within the last two years?

______(C) 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?

<u>Human Resources</u>

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

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

______ (C) Are employee accounts reviewed periodically for appropriate access?

______(C) 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?

______(C) 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?

<u>Physical Security</u>

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

______(C,A) Are appropriate environmental controls in place in the SaaS offering's data center(s)?

<u>Business Continuity and Disaster Recovery</u>

______ (A) How frequently is the SaaS offering's system/application backed up?

_______ (A) How frequently is our data backed up by the SaaS offering?

_______ (C) Are those backups encrypted?

_______ (A) Are those backups tested?

_______ (C,A) Are those backups performed or transported off-site?

_______(A) Will our organization have the ability to perform our own backups of our data from the SaaS offering?

_______ (A) How quickly can the SaaS offering recover from a catastrophic failure?

_______(A) How often are the business continuity and disaster recovery plans tested and reviewed?