Standard: Application Service Provider Security Requirements

Executive Summary

SJSU has the option to select and contract with approved 3rd parties, application service providers, services and software vendors. SJSU must take appropriate measures to ensure that these arrangements do not place its data at risk or weaken its information security to unauthorized disclosure. Application Service Provider Security Requirements standard defines the security requirements for application service providers for all SJSU computer and communication system information, with the goal of safeguarding the confidentiality, integrity, and availability of information stored, processed, and transmitted by SJSU.

Information Security Standards

Application Service Provider Security Requirements

Standard #	IS-ASPSR	Effective Date	11/10/2015	Email	security@sjsu.edu
Version	2.0	Contact	Mike Cook	Phone	408-924-1705

Revision History

Date	Action
5/31/2014	Draft sent to Mike
7/11/2014	QA Review
12/1/2014	Reviewed. Content suggestions. Added comments. Hien Huynh
3/2/2015	Reviewed. Constraints surround foreign entities removed. Mike Cook
11/10/2015	Incorporated changes from campus constituents – Distributed to Campus.

Table of Contents

Introduction and Purpose

This standard defines the security requirements for application service providers for all San Jose State University (SJSU) computer and communication system information, with the goal of safeguarding the confidentiality, integrity, and availability of information stored, processed, and transmitted by SJSU.

Scope

This standard applies to all SJSU State, Self-Fund, and Auxiliary ("campus") computer systems and facilities, with a target audience of SJSU Information Technology employees and partners.

Standard

3rd Party Risk Assessment & Audit Requirements

Cloud Security Questionnaire

All 3rd parties hosting level 1 sensitive information must complete the SJSU cloud security questionnaire. The Information Security Office will issue the cloud security questionnaire.

Risk Assessment Requirement

Information Owners that host sensitive level 1 information on 3rd party service providers will be responsible for undergoing an annual risk assessment, including an inventory of all applications and servers. Assignments will be made by the Information Security Office.

Service delivery

It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party. To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements. The organization should check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed with the third party.

Independent Control Reports

All agreements with information systems outsourcing organizations must stipulate that SJSU will annually receive a report expressing an independent opinion about the adequacy of the controls in use at the outsourcing organization.

Application Service Provider Software Escrow

Every application service provider handling SJSU production information must license the software to SJSU, periodically deposit the most recent version of the source code in an approved software escrow facility, and provide current detailed operational and procedural documentation.

Third Party Software Developers Access to Source Code

Third party programmers must not be granted unregulated access to SJSU source repositories. Only the modules needed for a specific programming task may be revealed to these programmers. These programmers must additionally never be given privileges to directly update SJSU production source or object code without authorization and without completion of a background check either by SJSU or by their employer (Consulting Firms).

Alternate Processing Provider

In every case where critical SJSU production information systems processing is handled by an outsourcing organization, an alternate provider must be ready to immediately take-over these activities if the outsourcing organization is no longer be able or willing to deliver on its promises.

Accessibility to Outsourced Information

In every case where SJSU uses an outsourcing organization to process or otherwise manage its production information, the contract with the outsourcing organization must clearly stipulate either for the daily delivery to SJSU of a complete and computer-readable copy of its information, or that SJSU has the right to immediately obtain a computer-readable copy of its information at any time and without limitation.

Access Control Decisions

Decisions about who will be granted access to both SJSU information and SJSU information systems must be made by SJSU management and never by outsourcing organization personnel.

Outsourcing Contract Approvals

All information-systems-related outsourcing contracts must be reviewed and approved by the Information Security Office who is responsible for ensuring that these contracts sufficiently define information security responsibilities, how to respond to a variety of potential security problems and the right to terminate the contract for cause if it can be shown that the outsourcing organization does not abide by the information-security-related contractual terms. Departments are responsible for obtain signed Confidentiality Agreements for third parties who are granted access to University data.

Outsourced Security Must Be At Least As Robust As In-House Security

The information security mechanisms to be used on a proposed outsourced system must be at least as strong and robust as those now found on the in-house systems used to perform these same production activities.

Remote Alarms Indicate Equipment Area Is Being Accessed

When outsourcing firms, such as Internet hosting firms and application service provider firms, are being employed, and where SJSU has its own equipment situated on the outsourcing firm's premises, a remote alarm system must be used. Such an alarm system must immediately report to SJSU staff when the door to a locked equipment area has been opened.

Privacy Audit on Third-Party Systems Storing Sensitive Information

SJSU reserves the right to perform a privacy audit on any third-party production system that stores sensitive information on customers or employees.

Managing changes to third party services

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

Outsourcing Firm Notice of Business and Technical Changes

Arrangements with information systems outsourcing firms must be structured such that Information Technology Department and Information Security Office management both receive notices of all material changes in the outsourcing firm business and technical environment. Such notices must be received well in advance of such changes actually taking effect.

Service Provider Contingency Plans

All contracts with web site hosting organizations, application service providers, managed systems security providers, and other information systems outsourcing organizations must include both a documented backup plan and a periodic third-party testing schedule.

Outsourced Production Systems Back-Out Plans

An effective and regularly-tested back-out plan, that permits SJSU to revert to internal processing and has been approved by the Information Security Office, must be prepared and tested before any production information system processing may be transferred to an outsourcing organization.