



## Stanford University ASP Preliminary Security Criteria & Questionnaire

### 1.0 Overview

This document defines the minimum security criteria that an Application Service Provider (ASP) must meet in order to be considered for use by Stanford University. As part of the ASP selection process, the ASP Vendor must demonstrate compliance with the Standards listed below by responding in writing to EVERY statement and question in the seven categories. We will closely review the vendor responses, and will suggest remediation measures in any areas that fall short of the minimum security criteria. Stanford University acceptance/approval of any given ASP's information security profile depends largely on the vendor's response to this document.

These Standards are subject to additions and changes without notice by Stanford University.

### 2.0 Scope

This document can be provided to ASPs that are either being considered for use by Stanford University, or have already been selected for use.

### 3.0 Responding to These Standards

Stanford University is looking for explicitly detailed, technical responses to the following statements and questions. ASPs should format their responses directly beneath the Standards (both questions and requirements) listed below. Please include any security whitepapers, technical documents or policies that you may have that may assist us in understanding your information security profile.

Answers to each Guideline should be specific and avoid generalities – <b>Examples:</b>
<i>Bad: "We have hardened our hosts against attack." Good: "We have applied all security patches for Windows 2000/2003 as of 4/30/2005 to our servers. Our Administrator is tasked with keeping up-to-date on current vulnerabilities that may affect our environment, and our policy is to apply new patches during our maintenance period (23:00hrs, Saturday) every week. Critical updates are implemented within 24 hours. A complete list of applied patches is available to Stanford University."</i>
<i>Bad: "We use encryption." Good: "All communications between our site and Stanford University will be protected by IPSec ESP Tunnel mode using 168-bit TripleDES encryption, SHA-1 authentication. We exchange authentication material via either out-of-band shared secret, or PKI certificates."</i>

## 4.0 Standards

### 4.1 General Security

1. Stanford University reserves the right to periodically audit the <ASP Company Name> application infrastructure pertaining to the environment hosting Stanford's applications/instance to ensure compliance with the Stanford Information Security Policies and these ASP Security Standards. Non-intrusive network audits (basic portscans, etc.) may be performed randomly, without prior notice. More intrusive network and physical audits may be conducted on site with 48 hours notice.
2. The ASP must provide a proposed architecture document that includes a full network diagram of the Stanford University Application Environment, illustrating the relationship between the Environment and any other relevant networks, with a full data flowchart that details where Stanford University data resides, the applications that manipulate it, and the security thereof.
3. The ASP must be able to immediately disable all or part of the functionality of the application should a security issue be identified. .
4. Please describe your Intrusion Detection Systems for both Host IDS and Network IDS.
5. Please describe your processes regarding security incident response. If you have documented Incident Response Guidelines or Polices, please provide that as well.
6. Does the ASP have a current Statement on Auditing Standards (SAS) 70 Report? If so, who performed the audit?
7. If the ASP does not have a current SAS 70 Report, does the ASP meet other certified standards? (Please list the certification standard met, e.g. BSO, ISO, CMM, PCI and who performed the certification.) The ASP shall provide Stanford copies of current and subsequent certifications. During the contract period, the ASP shall disclose to Stanford any material weaknesses, or deficiencies identified during audits on the Vendor facilities hosting, or data pathways, supporting Stanford projects.

### 4.2 Physical Security

1. The equipment hosting the application for Stanford University must be located in a physically secure facility, which requires badge access at a minimum.
2. The infrastructure (hosts, network equipment, etc.) hosting the Stanford University application must be located in a locked cage-type environment.
3. If Stanford University Infrastructure is hosted, Stanford shall have final say on who is authorized to enter the physical environment containing the Application Infrastructure.
4. The ASP must disclose their access control procedures, including who amongst their personnel (by roles) will have access to the environment hosting the application for Stanford University and the ASP's user administration processes.
5. Stanford University requires that the ASP disclose their employee/contractor background check procedures and results prior to Stanford University granting approval for use of an ASP.

### 4.3 Network Security

1. Stanford University requires that the network hosting the production and development environments be on separate (air-gapped) networks from each other.
2. Stanford University prefers that the network hosting the production application and data be air-gapped from any other network or customer that the ASP may have. If this is difficult to achieve within the ASP architecture, then please describe how Stanford's data is segregated from the data of other customers.
3. Stanford University requires access to any security, traffic or authentication logs relating to the access and connectivity to the University's application and development environments.
4. How will data travel between Stanford University and the ASP? Keep in mind the following three points:
  - a. If Stanford University will be connecting to the ASP via a private circuit (such as frame relay, etc.), then that circuit must terminate on the Stanford University extranet, and the operation of that circuit will come under the procedures and policies that govern the Stanford University eCommerce Systems Management Group.
  - b. If, on the other hand, the data between Stanford University and the ASP will traverse a public network such as the Internet, the ASP must deploy appropriate firewalling technology, and the traffic between Stanford University and the ASP must be protected and authenticated by cryptographic technology (See Cryptography §4.6 below). Stanford University requires administrative access to any firewalls and/or routers on the University's side of the firewall infrastructure.
  - c. No "split-tunneling" of any secure connection between the ASP and Stanford University.

### 4.4 Host Security

1. The ASP must disclose how and to what extent the hosts (Unix, Linux, Windows, etc.) comprising the Stanford University application infrastructure have been hardened against attack. If the ASP has documentation for its hardening standards and processes, please provide that as well.
2. The ASP must provide a listing of current patches on hosts, including host OS patches, web servers, databases, and any other material application.
3. Information on how and when security patches will be applied must be provided. How does the ASP keep up on security vulnerabilities, and what is the policy for applying security patches?
4. The ASP must disclose their processes for monitoring the integrity and availability of those hosts.
5. The ASP must provide information on their password policy for the Stanford University application infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.
6. Stanford University cannot provide internal usernames/passwords for account generation, as the company is not comfortable with internal passwords being in the hands of third parties. With that restriction, how will the ASP authenticate users? (e.g., LDAP, Netegrity, Client certificates.)
7. The ASP must provide information on the account generation, maintenance and termination process, for both maintenance as well as user accounts. Include information as to how an account

is created, how account information is transmitted back to the user, and how accounts are terminated when no longer needed.

#### **4.5 Web Security**

1. At Stanford University's discretion, the ASP may be required to disclose the specific configuration files for any web servers and associated support functions (such as search engines or databases).
2. Please disclose whether, and where, the application uses Java, JavaScript, ActiveX, PHP or ASP (active server page) technology.
3. What language is the application back-end written in? (C, Perl, Python, VBScript, etc.)
4. Please describe the ASP process for doing security Quality Assurance testing for the application. For example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture.
5. Has the ASP performed a web code review, including CGI, Java, etc, for the explicit purposes of finding and remediating security vulnerabilities? If so, who did the review, what were the results, and what remediation activity has taken place? If not, when is such an activity planned?

#### **4.6 Cryptography**

1. The Stanford University application infrastructure cannot utilize any "homegrown" cryptography – any symmetric, asymmetric or hashing algorithm utilized by the Stanford University application infrastructure must utilize algorithms that have been published and evaluated by the general cryptographic community.
2. Encryption algorithms must be of sufficient strength to equate to either, 168-bit TripleDES or 128-bit AES.
3. Connections to the ASP utilizing the Internet must be protected using any of the following cryptographic technologies: IPSec, SSL, SSH/SCP.
4. If the Stanford University application infrastructure requires PKI, please contact Stanford University Information Security Office for additional guidance.

#### **4.7 eCommerce**

1. If the ASP solution concerns any electronic commerce activities the following questions must be addressed:
2. Describe the protections for any transaction web pages hosted.
3. Is any customer credit card information collected and/or stored?
4. If credit card information is stored, is this information stored in an encrypted or otherwise protected manner?
5. Is the application certified PCI – DSS compliant? (Please list the date(s) the certification standards were met, and who performed the certification.) The ASP shall provide Stanford copies of current and subsequent certifications.
6. Is the ASP Vendor certified PCI-DSS compliant? Is the ASP a Tier 1, 2, 3 or 4 level eTransaction merchant, for CISP classification purposes. (Please list the date(s) the certification standards were

met, and who performed the certification.) The ASP shall provide Stanford copies of current and subsequent certifications.

## 5.0 Security - Other

1. Many of the applications and systems considered for this ASP contain restricted, sensitive and private information, which the University is required to protect. Stanford is mandated to maintain its ability to ensure tight controls over the production and development environments and the information contained the databases.
2. Required Contract Clauses – Stanford’s Procurement Office must be notified if the applications and systems considered for this ASP handle or store University Restricted, Sensitive and private information, so that appropriate contract language is included. Examples of specific contract addendums typically used by Stanford are:
  - Credit Card Privacy – PCI Compliance Addendum
  - FERPA – FERPA Addendum
  - Financial – Confidential Financial Information Addendum
  - HIPAA – Business Associate Agreement
  - General – Non-Disclosure Agreement
  - Insurance – Insurance Requirements

## 6.0 Security – Background & Additional Information

1. Information Security Drivers - Stanford University is committed to protecting its information resources from accidental or intentional intrusion or damage and is equally committed to preserving and nurturing the open, information-sharing requirements of its academic culture. . Protecting information assets is driven by a variety of considerations including legal, academic, financial and other business requirements.
  - Legal - There are laws, both federal (e.g., HIPAA, FERPA) and state (e.g., social security number use, credit card exposure), that affect the level of protection Stanford is required to provide. Stanford also has many contractual relationships around the protection of data that is licensed from other sources.
  - Academic - Stanford both produces and owns intellectual capital, which needs to be protected against premature disclosure, or unauthorized tampering.
  - Financial - There are costs directly related to the protection of information assets. Similarly, there are costs directly related to the control and repair of damage to information resources that have been compromised.
  - Other business requirements - While Stanford, as a part of its fundamental mission, wants to make sure that many information resources are widely available it also wants to keep private things private. Moreover, in addition to the direct costs related to damage control, Stanford's reputation as a world-class institution is something that, if damaged, can have both direct and indirect negative effects.
2. Stanford University Administrative Guide Memos (Policies) on Computing - <http://adminguide.stanford.edu/ch6contents.html>
3. Data Classification – Matrix regarding Stanford University’s Data Classification Schema described in Administrative Guide Memo #63, Information Security and in - [http://www.stanford.edu/group/security/securecomputing/dataclass\\_chart.html](http://www.stanford.edu/group/security/securecomputing/dataclass_chart.html)
4. Information Security: Guidelines for Applications - <http://www.stanford.edu/group/security/securecomputing/iso-guidelines.html>