Application Service Providers (ASP) Policy

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose
This document describes Information Security's requirements of Application Service Providers (ASPs) that engage with <Company Name>.

2.0 Scope
This policy applies to any use of Application Service Providers by <Company Name>, independent of where hosted.

3.0 Policy
3.1 Requirements of Project Sponsoring Organization
The ASP Sponsoring Organization must first establish that its project is an appropriate one for the ASP model, prior to engaging any additional infrastructure teams within <Company Name> or ASPs external to the company. The person/team wanting to use the ASP service must confirm that the ASP chosen to host the application or project complies with this policy. The Business Function to be outsourced must be evaluated against the following:

1. The requester must go through the ASP engagement process with the ASP Tiger Team to ensure affected parties are properly engaged.
2. In the event that <Company Name> data or applications are to be manipulated by, or hosted at, an ASP's service, the ASP sponsoring organization must have written, explicit permission from the data/application owners. A copy of this permission must be provided to InfoSec.
3. The information to be hosted by an ASP must fall under the "Minimal" or "More Sensitive" categories. Information that falls under the "Most Sensitive" category may not be outsourced to an ASP. Refer to the *Information Sensitivity Policy* for additional details.
4. If the ASP provides confidential information to <Company Name>, the ASP sponsoring organization is responsible for ensuring that any obligations of confidentiality are satisfied. This includes information contained in the ASP's application. <Company Name>'s legal services department should be contacted for further guidance if questions about third-party data arise. Projects that do not meet these criteria may not be deployed to an ASP.

3.2 Requirements of the Application Service Provider
InfoSec has created an associated document, entitled *ASP Security Standards* that sets forth the minimum security requirements for ASPs. The ASP must demonstrate compliance with these Standards in order to be considered for use.

The ASP engagement process includes an InfoSec evaluation of security requirements. The *ASP Security Standards* can be provided to ASPs that are either being considered for use by <Company Name>, or have already been selected for use.

InfoSec may request that additional security measures be implemented in addition to the measures stated in the *ASP Security Standards* document, depending on the nature of the project. InfoSec may change the requirements over time, and the ASP is expected to comply with these changes.

ASPs that do not meet these requirements may not be used for <Company Name> Systems, Inc. projects.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Application Service Providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

5.0 Definitions

Terms	**Definitions**
Application Service Provider (ASP)	ASPs combine hosted software, hardware and networking technologies to offer a service-based application, as opposed to a <Company Name>-owned and operated application. Common ASP offerings include enterprise resource planning (ERP), collaboration and sales force automation tools, but are not limited to these things.
ASP Sponsoring Organization	The group within <Company Name> that wishes to utilize the services of an ASP.
Business Function	The business need that a software application satisfies. managed by an ASP that hosts an application on behalf of <Company Name>.

6.0 Revision History