Sample Third Party Management Policy

Establishment date, effective date, and revision procedure

This policy was established and approved by [*Organization Name*] on mm,dd,yyyy. The [*Organization Name*] Information Security department of shall review this policy at least once a year, and at any additional time when there are changes that may affect corporate management with respect to Information Security. In the event that amendment or repeal of this policy becomes necessary as a result of such review, the [*Organization Name*] Information Security department shall prepare a draft and apply for authorization, and with prior confirmation of the Corporate Executive(s) in charge of the area(s) that will be affected by amendment or repeal, the [*Organization Name*] CISO/Security Director will authorize the amendment or repeal.

Table of revision history

Version	Date	Details of change	Issued by	Approved by

Introduction

Purpose

The purpose of this policy is to set forth security requirements to be observed by all employees who are responsible for managing relationships with third parties throughout the organization.

Scope

The scope of this policy shall be the same as the scope of [*Organization Name's*] Security Policy.

Applicability

This policy applies to employees who are responsible for managing relationships with third parties.

Definitions

- *Sensitive information*. Secret information and/or confidential.
- *Third Parties*. External parties which include, but are not limited to,
    - Business partners;
    - Customers; and
    - Contractors (e.g. (i) service providers, such as ISPs, network providers, telephone services, maintenance and support services, (ii) managed security services, (iii) outsourcing of facilities and/or operations, e.g. IT systems, data collection services, call center operations, (iv) business consultants and auditors, (v) developers and suppliers, e.g. software products and IT systems, (vi) cleaning, catering, and other outsourced services, (vii) temporary personnel, student placement, and other casual short-term appointments)

Confidentiality Agreement

Where there is a business need to disclose any sensitive information of [*Organization Name*] to third parties (such as business partners and contractors), or grant third parties access to sensitive information, the management of [*Organization Name*] must execute a confidentiality agreement or an agreement that incorporates confidentiality provisions with such third parties in advance.

It is prohibited for the employees of [*Organization Name*] to disclose sensitive information to a third party or to grant a third party access to sensitive information, without execution of a confidentiality or similar agreement.

Requirements of the Confidentiality Agreement

Security requirements must be identified and incorporated in the confidentiality or similar agreement, based on the confidentiality of the information.

The following requirements shall be incorporated in the confidentiality or similar agreement as fundamental obligations of the third party that has possession of [*Organization Name*] sensitive information.

A. It shall strictly keep in confidence and not disclose or disseminate to any other party the sensitive information and shall not use the sensitive information without [*Organization Name*] prior written consent for any purpose other than those stipulated in the confidentiality or similar agreement. (Third parties' obligations of confidentiality shall be perpetual as to the confidential information for which any laws/regulations provide specific requirements, such as personal information).

B. In order to protect sensitive information, the recipient shall undertake the following:

1. Not to make any copy or reproduction of the sensitive information without [*Organization Name*] prior consent (exceptions may be required, such as in the case of authorized external lawyers using [*Organization Name*] materials);
2. To use the same degree of care in protecting the confidentiality of the sensitive information as the receiving party would use to protect its own confidential and proprietary information of a similar nature (but in any event, no less than a reasonable degree of care, or as required by law), to avoid disclosure, publication or dissemination of the information, including all derivative materials that the receiving party would produce or make during the course of the usage of the sensitive information; and
3. Without limiting any of the foregoing obligations: i) to use a secure method (e.g. encryption) when transmitting sensitive information; ii) to ensure that [*Organization Name*] sensitive information is not commingled with any other organization's confidential information and iii) to notify [*Organization Name*] of any suspected, potential or actual breach of security or other exposure involving sensitive information.

C. If requested by [*Organization Name*], the recipient shall promptly return or destroy all sensitive information in its possession in a secure manner and shall provide [*Organization Name*] with a declaration to that effect in a form satisfactory to [*Organization Name*], duly executed.

D. The recipient shall permit personnel designated by [*Organization Name*] to review the recipient's security procedures for the protection of sensitive information at least annually (during normal business hours or otherwise at such parties' consent). At [*Organization Name's*] option, such review may include, without limitation, performing penetration testing and vulnerability scans, observing operations, reviewing documents and other materials, and interviewing relevant personnel of the recipient. If, upon such review, [*Organization Name*] determines that the recipient is not in compliance with the terms agreed, [*Organization Name*] shall so notify the recipient in writing of such non-compliance. In the event of such non-compliance, [*Organization Name*] shall have the right to terminate its agreement with the recipient and to take other actions and seek such remedies as appropriate under the circumstances.

Management of Third Party Services

Third-Party Qualifications

All potential third-party service agreements that include the disclosure of, or access to, sensitive information as described in the Confidentiality Agreement must include the Confidentiality Agreement requirements outlined in this policy.

Depending on individual circumstances, the business unit may choose to review the information security practices of the third party. Sample checklists and questionnaires are provided in the appendices as one means of conducting this review.

Service Agreement

The employee responsible for managing the third party must define specific procedures to ensure that, before work starts, a service agreement is defined and executed, and that it conforms to the security standards of [*Organization Name*] in accordance with legal and regulatory requirements.

Observation of [*Organization Name*] Rules

Where the services are performed at [*Organization Name's*] premises, the employee responsible for managing the third party must have the third party service providers observe and agree to comply with

rules related to information security while on [*Organization Name's*] premises, and obtain from them a written undertaking to observe the rules adopted for the relevant [*Organization Name*] premises.

Third Party Access

Access to sensitive information on [*Organization Name*] premises must only be granted to third parties in controlled circumstances and must be approved with clear reference to the reason why access is necessary. These reasons include approved on-site maintenance or where specialist support is required with access to systems and/or premises. Examples of on-site third parties include

- Hardware and software maintenance and support staff;
- Cleaning, catering, security guards and other outsourced support services;
- Student placement and other casual short-term appointments; or
- Consultants.

External Connectivity Process

In a case where there is a requirement to connect the network of a third party with [*Organization Name's*] network, business and technical reasons for requiring such a connection must be documented and a full risk assessment must be completed and approved by [*Organization Name's*] IT Department or appropriate delegated authority, and the documentation and the approved risk assessment must be retained for audit purposes.

APPENDIX A: Sample Security Checklist

Pre-Assessment Security Checklist	Y/N	Comments
1. Has a non-disclosure agreement (NDA) been signed/executed between the parties? (Y/N)		
2. Identify where the risk is located (external, internal) • Are there architecture items residing outside [*Organization Name's*] Corporate Network? • Are there architecture items residing inside the [*Organization Name*] Corporate Network?		
3. Has this application/web service/request location had a Security Audit Previously? • If so, can the vendor provide a summary under NDA? • Has the architecture/environment changed since previous audit?		
4. Which kind of information will be included in this application/web service/ request? Does it include [*Organization Name's*] confidential information?		
5. User access to the application/web service/request is understood • [*Organization Name*] manages the user access controls (create, modify, delete process) • Business Partners manage user access controls • End User manages user access controls		

APPENDIX B: Sample Connection Request Form

EXAMPLE: [*Organization Name*] External Connection Request Form

As [*Organization Name*] is extending and outsourcing its business operations, service and support using external network connections to third parties, IT Infrastructure and Security need to be able to determine the levels of risk and controls required to protect [*Organization Name's*] confidential property. A security assessment form must be completed before a network connection proposal is approved. This is mandatory for all links (including VPN or SSL via the Internet) to third parties, Joint Ventures and any alliances linked to any [*Organization Name*] site or facility.

Business Scope & Requirements

- Briefly describe how the connection will support existing or planned business needs (e.g. when it is needed, how long it is needed for, and how it will be used).

- Describe the business relationship between the two organizations. Does a contract already exist between the two organizations, and if so, please provide details of the contract number and name and email address of the contract administrator. All contracts must contain intellectual property rights clauses which cover organizations, their employees and all sub-contractors, together with non-disclosure agreements including data privacy clauses signed by their organization director and all individuals who have network access into [*Organization Name*] or are allowed to view [Organization Name's] intellectual property.

- List [*Organization Name*] staff involved with the connection project, including the Business Manager, Project Sponsor, and the Project Manager. List all of [*Organization Name*] parties involved in the installation and support of this connection, including technical contacts. Provide email addresses and phone numbers.

[Organization Name's] Personnel	Department	Project Role	Telephone Number	Email Address
Business Sponsor				

The organization personnel involved with the connection project are as follows;

Name	Department	Project Role	Telephone Number	Email Address
Business Sponsor				

- Record the sensitivity of the most sensitive data that will traverse the network boundary. Identify the classification for [*Organization Name*] information which will be in the custody of the other organization. If sensitive information of the other organization is in [*Organization Name's*] possession, please state the equivalent [*Organization Name*] data classification. (Consider the business risk should their data be made public.)

- If any personal information (employee or consumer) is being collected or processed, please provide the personal data elements and details of where the personal data will be stored, and where it be accessed from. (Country, location, etc.)

- Note the quality of service and criticality (availability) of information and services that will be available via the connection.

- Please provide any other pertinent information that was not included in the above responses (e.g. outsourcing details and plans)

Technical Requirements

Complete this section in collaboration with the networking team. Be prepared to discuss and then document the following:

- Diagram the hardware involved (e.g. computers, routers, LAN segments, data circuits, etc.) at each site. This diagram should depict the entire proposed network architecture, including all connections to other networks. Show the physical location of each element and note who will have physical access, and how physical access will be controlled.

- Record the proposed connection method that will be used between the networks or sites. Explain how connections will be initiated and authenticated.

- Note the transport protocol(s) (TCP/IP, etc.) that will carry traffic across the network(s).

- Show where each software program/module will reside (client, server, user agent, gateway/proxy, database, etc.). Include information about the operating system and network services provided by each computer.

- Note the application protocols to be used to move data and control/monitor the systems (i.e.: WWW, SQL, SSL, FTP, SMTP, SNMP, DNS, ping, etc.). Assume all application protocols are denied by the firewall by default; therefore list every protocol and port that will be needed. Describe how the sessions or accesses are initiated and authenticated. For each application protocol listed, identify each pair of hosts that will be utilizing that application protocol. For commercial application protocols (e.g. SQL), please provide vendor documentation. If a security certificate is to be used, please provide details. Please include details of remote printing.

- For proprietary application protocols, describe the security controls and integrity checks that are provided. For each proprietary application protocol, please provide the protocol specification.

- Intrusion Detection/Prevention Services (IDS or IPS) are required to be installed and monitored real time 24 x 7 hours. Explain how these services will be monitored, and by whom.

- Determine the predicted end-to-end end network traffic. What is the typical or average number of bytes per transaction per unit time? Does the application require a minimum network latency, or reserved bandwidth?

- Describe how each computer and application will be managed/administered, physically secured, logged, etc. Will there be restricted or controlled physical access?

- For applications that are already in use, who currently has access? (e.g. for a database application, who has database access today?) Please describe the architecture of the application by providing as much documentation as possible.

- What are the future requirements of this connection (e.g. protocols, other entities, bandwidth, growth, etc.)

APPENDIX C: Security Questionnaire

EXAMPLE: Information Security Assessment Questionnaire for ASPs, ISPs, and Other Service Providers

Executive Summary

As the organization moves to an outsourcing environment, and offsite hosting for our eBusiness web sites and services, the business organizations and application owners must ensure that they have performed a risk assessment to protect our eBusiness from any damage to our brand. It is critical to ensure that all hosting companies provide "best practices" in their security processes and policies. By insisting upon best industry practices (ISO27000 series or BS7799) we will ensure that we can provide excellent customer service by maintaining the accuracy, the privacy and the availability of our eBusiness web sites for our customers, both internally and externally.

This baseline questionnaire provides the criteria to evaluate the level of information protection offered by Internet Service Providers (ISPs), Application Service Providers (ASPs) or other vendors that provide eBusiness services. It is designed as a tool for [Organization Name] project managers, application/business owners and IT support managers to evaluate the key information protection practices of companies providing eBusiness services. The questionnaire encompasses their basic security practices and standards, their willingness to provide proof of their trustworthiness, and their capability to provide services to keep clients informed of security vulnerabilities and fixes.

Business Objectives

The business organizations and applications owners must conduct a risk assessment in coordination with [*Organization Name*] Security and Infrastructure Services to ensure that minimum security standards and best practices are followed by the ISP/ASP/other service providers. The objective is to take proactive steps to ensure we protect [*Organization Name*] brand equity in the eBusiness marketplace. This objective must include assurance that the vendor has processes in place to prevent, identify, and correct any potential security vulnerabilities that could be exploited, including web defacement, denial of service attacks, fraudulent transactions, inserting Trojan horse code/malicious code, unauthorized use of site hosts, eavesdropping, inadvertent disclosure of confidential information, and other exploitations.

[*Organization Name*] eBusiness application/business owners must understand that the ISPs/ASPs/other service providers often provide different levels of security on a customizable basis, with various security services being offered a la carte. [*Organization Name*] clients need to ask about the availability and pricing of each and every security service they need based on the level of business risk that is acceptable to that business unit.

APPENDIX D: Information Security Assessment

EXAMPLE: Information Security Assessment Questionnaire:

Guideline Questions to Evaluate Service Providers

The various factors to be considered in evaluating the security capabilities of service providers are based on industry benchmarking for “best practices” in the level of security services and controls provided by a company. Each factor has an impact on the overall security assurance provided by an Internet service provider (ISP), application service provider (ASP), or other type of service provider.

When selecting an eBusiness vendor, the business unit should consider each of these factors in weighing the overall risk to the eBusiness application and/or service.

Guideline Questions for Evaluation of Information Protection Practices/Policies/Standards		**Y/N**	**Provide Explanations/Details as Appropriate**
1	Is the hosting facility certified to BS7799 or ISO27000 series standards, and can [*Organization Name*] perform an audit to evaluate the hosting facility?		
2	Can [*Organization Name*] perform site penetration and vulnerability testing of the hosting facility?		
3	Is Vendor infrastructure evaluated through external penetration tests on at least a quarterly basis?		
4	Is Vendor internal network security audited at least annually by an independent audit/security assessment company with industry-recognized expertise in this field?		
5	Does Vendor perform their own internal network security audits and conduct their own external penetration and vulnerability tests at least quarterly, based on best practices in the industry?		
6	Does Vendor have documented firewall configuration standards?		
7	Does Vendor have documented firewall administrative procedures and regular audit log review?		
8	Does Vendor require two-factor authentication for administrative control of all routers, firewall and eBusiness application servers?		
9	A. Is all access to application and supporting computer/networks logged (including access by system administrators, operators, development or audit staff)? B. Are these logs retained for a minimum period of 8 weeks? C. Are these logs regularly monitored? D. Are these logs unalterable (e.g. use write-once technology or equivalent protection)?		
10	A. Is intrusion detection/monitoring for customers provided with comprehensive, documented reporting processes and escalation procedures? (Includes application or transaction-based intrusion detection) B. Are there proactive processes/measures in place to protect against web defacement attacks? Explain. C. Are there proactive processes/measures in place to protect against distributed denial of service attacks? Explain.		

11	Are incident response, security incident escalation procedures and emergency staff contacts (includes 24X7 contacts) all documented and kept current?		
12	Are there documented help desk procedures for authenticating callers and resetting access controls?		
13	A. Are administrative accounts rigorously controlled with a very minimum number per system? B. Are there standards for strong password composition and a minimum length of 10-12 characters?		
14	Is Encryption (256-bit) used to protect the confidentiality of transmitted information, especially for payment systems and personal information?		
15	Is encryption and two-factor authentication supported for the connection from [*Organization Name*] LAN to the Vendor's backbone?		
16	Do sensitive materials have special controls to ensure their secure storage, transport and disposal? Explain.		
17	A. Are security policies documented and made available for review? B. Are security requirements/practices for maintaining security documented and comprehensive? Please make copies available for review during site visit.		
18	A. Is a privacy policy documented and published? Please provide a copy. B. Does the policy strictly prohibit the sale, the rental, the transfer, the trading of or the disclosure otherwise of [Organization Name] or customers' personal information to third parties without such customer's consent? C. Does this prohibition include NOT treating the customer information as a business asset during a potential merger or acquisition?		
19	A. How does the security officer rank within the Vendor organization? B. Please provide a hierarchical diagram of the security organization. C. Is security staffing comprehensive and are there clearly defined Roles and Responsibilities? D. How are security incidents reported within and outside of the security organization? E. Does the vendor notify [Organization Name] of a security incident within one hour of knowledge of the reported occurrence? F. Does the vendor provide logs and data about the incident to [*Organization Name*] for investigation and validation of the vendor's findings? Is this done within 3 hours of the occurrence of the incident? Please provide details of the flow of responsibility within the organization for all security incident reporting.		
20	Does the Vendor perform background checks on staff that will have administrative access to critical servers/applications/networks/infrastructure?		
21	A. Do the security staff have an average of more than 3 years of experience in information/network security? B. Does approximately 75% of the security staff have CISSP or other security industry certification?		

22	Are proper education and training provided to the security staff and employees in charge of information security activity?		
23	A. Are there special distinguishing security features, such as caged equipment rooms or biometrically controlled vaults? B. Is this included in your basic service price or is it provided at an additional cost to [*Organization Name*]?		
24	A. Are there “hot standbys” for all components of the eBusiness application that are critical to the continuity of the applications/services? This should include both redundancy and load-balancing services for all security critical elements. B. Is this included in your basic service price or is it provided at an additional cost to [*Organization Name*]?		
25	If the vendor relies on third party services, is there a detailed service-level agreement between the Vendor and their own providers? Please provide a copy of your generic SLA template.		
26	A. Are there documented standards and processes for critical system components to ensure the evaluation and installation of vendor-issued updates and patches to remove/correct known security problems? Please provide example of processes for review at site visit. B. Are high-risk vulnerability patches applied within 7 days? C. Is the Vendor a member of the Forum of Incident Response and Security Teams (or uses a security service provider that is a member)?		
27	A. Are there documented security standards regarding server OS hardening and are they rigorously enforced? Please provide examples for review during site visit. B. Explain tools used for enforcement.		
28	Are there documented processes to ensure that the software products, computers and networks that support the eBusiness application are up-to-date versions?		
29	Are there documented security standards and audit procedures for the customer network security to ensure that customers cannot compromise the Vendor backbone? Please provide processes and standards for review during site visit.		
30	Are there documented controls to ensure separation of data and security information between customer applications if the Vendor co-locates customer applications on physical servers? Please provide processes for review during site visit.		