

ISO 27001 security

Information Security Policy

on

Outsourcing

Summary

This policy mandates the assessment and management of commercial and information security risks associated with business process outsourcing.

Outsourcing security policy

Index

1	Introduction	3
2	Objective.....	3
3	Scope	3
4	Axioms	4
5	Policy statements.....	4
5.1	Choosing an outsourcer.....	4
5.2	Assessing outsourcing risks	4
5.3	Contracts and Confidentiality Agreements.....	5
5.4	Hiring and Training	7
5.5	Access Control	8
5.6	Security audits	9
6	Responsibilities.....	9
6.1	Management.....	9
6.2	Outsourced business process owners	9
6.3	Information Security.....	10
6.4	Internal Audit	10
7	Copyright	10
8	Disclaimer.....	10

Version	Issue Date	Prepared by	Approved by	Description
1	23 rd March 2008	Aaron d'Souza and Gary Hinson		Generic sample policy published at www.ISO27001security.com

1 Introduction

- 1.1.1 Outsourcing involves transferring responsibility for carrying out an activity (previously carried on internally) to an outsourcer for an agreed charge. The outsourcer provides services to the customer based on a mutually agreed service level, normally defined in a formal contract.
- 1.1.2 Many commercial benefits have been ascribed to outsourcing, the most common amongst these being:
- Reducing the organization's costs
 - Greater focus on core business by outsourcing non-core functions
 - Access to world-class skills and resources
- 1.1.3 Despite the potential benefits, information security incidents such as inappropriate access to or disclosure of sensitive information, loss of intellectual property protection or the inability of the outsourcer to live up to agreed service levels, would reduce the benefits and could jeopardize the security posture of the organization.

2 Objective

- 2.1.1 This policy specifies controls to reduce the information security risks associated with outsourcing.

3 Scope

- 3.1.1 The policy applies throughout <ORGANIZATION>.
- 3.1.2 Outsourcing providers (also known as outsourcers) include:
- hardware and software support and maintenance staff
 - external consultants and contractors
 - IT or business process outsourcing firms
 - temporary staff
- 3.1.3 The policy addresses the following controls found in the ISO/IEC 27002:2005 and ISO/IEC 27001 standards:
- 6.2.1 Identification of risks related to external parties
 - 6.2.2 Addressing security when dealing with customers
 - 6.2.3 Addressing security in third party agreements

4 Policy axioms

- 4.1.1 The commercial benefits of outsourcing non-core business functions must be balanced against the commercial and information security risks.
- 4.1.2 The risks associated with outsourcing must be managed through the imposition of suitable controls, comprising a combination of legal, physical, logical, procedural and managerial controls.

5 Policy statements

5.1 Choosing an outsourcer

- 5.1.1 Criteria for selecting an outsourcer shall be defined and documented, taking into account the:
- company's reputation and history;
 - quality of services provided to other customers;
 - number and competence of staff and managers;
 - financial stability of the company and commercial record;
 - retention rates of the company's employees;
 - quality assurance and security management standards currently followed by the company (e.g. certified compliance with ISO 9000 and ISO/IEC 27001).
- 5.1.2 Further information security criteria may be defined as the result of the risk assessment (see next section).

5.2 Assessing outsourcing risks

- 5.2.1 Management shall nominate a suitable <ORGANIZATION> owner for each business function/process outsourced. The owner, with help from the local Information Risk Management Team, shall assess the risks before the function/process is outsourced, using <ORGANIZATION>'s standard risk assessment processes.

Outsourcing security policy

- 5.2.2 In relation to outsourcing, specifically, the risk assessment shall take due account of the:
- a) nature of logical and physical access to <ORGANIZATION> information assets and facilities required by the outsourcer to fulfill the contract;
 - b) sensitivity, volume and value of any information assets involved;
 - c) commercial risks such as the possibility of the outsourcer's business failing completely, or of them failing to meet agreed service levels or providing services to <ORGANIZATION>'s competitors where this might create conflicts of interest; *and*
 - d) security and commercial controls known to be currently employed by <ORGANIZATION> and/or by the outsourcer.
- 5.2.3 The result of the risk assessment shall be presented to management for approval prior to signing the outsourcing contract. Management shall decide if <ORGANIZATION> will benefit overall by outsourcing the function to the outsourcer, taking into account both the commercial and information security aspects. If the risks involved are high and the commercial benefits are marginal (e.g. if the controls necessary to manage the risks are too costly), the function shall not be outsourced.

5.3 Contracts and confidentiality agreements

- 5.3.1 A formal contract between <ORGANIZATION> and the outsourcer shall exist to protect both parties. The contract shall clearly define the types of information exchanged and the purpose for so doing.
- 5.3.2 If the information being exchanged is sensitive, a binding confidentiality agreement shall be in place between <ORGANIZATION> and the outsourcer, whether as part of the outsource contract itself or a separate non-disclosure agreement (which may be required before the main contract is negotiated).
- 5.3.3 Information shall be classified and controlled in according with <ORGANIZATION> policy.
- 5.3.4 Any information received by <ORGANIZATION> from the outsourcer which is bound by the contract or confidentiality agreement shall be protected by appropriate classification and labeling.
- 5.3.5 Upon termination of the contract, the confidentiality arrangements shall be revisited to determine whether confidentiality has to be extended beyond the tenure of the contract.

Outsourcing security policy

5.3.6 All contracts shall be submitted to the Legal for accurate content, language and presentation.

5.3.7 The contract shall clearly define each party's responsibilities toward the other by defining the parties to the contract, effective date, functions or services being provided (e.g. defined service levels), liabilities, limitations on use of sub-contractors and other commercial/legal matters normal to any contract. Depending on the results of the risk assessment, various additional controls should be embedded or referenced within the contract, such as:

- Legal, regulatory and other third party obligations such as data protection/privacy laws, money laundering *etc.* *;
- Information security obligations and controls *such as*:
 - Information security policies, procedures, standards and guidelines, normally within the context of an Information Security Management System such as that defined in ISO/IEC 27001;
 - Background checks on employees or third parties working on the contract (see [section 5.4](#));
 - Access controls to restrict unauthorized disclosure, modification or destruction of information, including physical and logical access controls, procedures for granting, reviewing, updating and revoking access to systems, data and facilities *etc.*(see [section 5.5](#));
 - Information security incident management procedures including mandatory incident reporting;
 - Return or destruction of all information assets by the outsourcer after the completion of the outsourced activity or whenever the asset is no longer required to support the outsourced activity;
 - Copyright, patents and similar protection for any intellectual property shared with the outsourcer or developed in the course of the contract;
 - Specification, design, development, testing, implementation, configuration, management, maintenance, support and use of security controls within or associated with IT systems, plus source code escrow;
 - Anti-malware, anti-spam and similar controls;
 - IT change and configuration management, including vulnerability management, patching and verification of system security controls prior to their connection to production networks;

* In the case of "offshore" outsourcing, special consideration must be given to the ramifications of transferring information between countries or jurisdictions, particularly where privacy and similar laws may conflict. Take qualified legal advice as a matter of course.

Outsourcing security policy

- The right of <ORGANIZATION> to monitor all access to and use of <ORGANIZATION> facilities, networks, systems *etc.*, and to audit the outsourcer's compliance with the contract, or to employ a mutually agreed independent third party auditor for this purpose;
- Business continuity arrangements including crisis and incident management, resilience, backups and IT Disaster Recovery.

5.3.8 Although outsourcers that are certified compliant with ISO/IEC 27001 can be presumed to have an effective Information Security Management System in place, it may still be necessary for <ORGANIZATION> to verify security controls that are essential to address <ORGANIZATION>'s specific security requirements, typically by auditing them (see [section 5.6](#)).

5.4 Hiring and training of employees

5.4.1 Outsource employees, contractors and consultants working on behalf of <ORGANIZATION> shall be subjected to background checks equivalent to those performed on <ORGANIZATION> employees. Such screening shall take into consideration the level of trust and responsibility associated with the position and (where permitted by local laws):

- Proof of the person's identity (*e.g.* passport);
- Proof of their academic qualifications (*e.g.* certificates);
- Proof of their work experience (*e.g.* résumé/CV and references);
- Criminal record check;
- Credit check.

5.4.2 Companies providing contractors/consultants directly to <ORGANIZATION> or to outsourcers used by <ORGANIZATION> shall perform at least the same standard of background checks as those indicated above.

5.4.3 Suitable information security awareness, training and education shall be provided to all employees and third parties working on the contract, clarifying their responsibilities relating to <ORGANIZATION> information security policies, standards, procedures and guidelines (*e.g.* privacy policy, acceptable use policy, procedure for reporting information security incidents *etc.*) and all relevant obligations defined in the contract.

5.5 Access controls

5.5.1 In order to prevent unauthorized access to <ORGANIZATION>'s information assets by the outsourcer or sub-contractors, suitable security controls are required as outlined in this section. The details depend on the nature of the information assets and the associated risks, implying the need to assess the risks and design a suitable controls architecture.

5.5.2 Technical access controls shall include:

- User identification and authentication;
- Authorization of access, generally through the assignment of users to defined user rôles having appropriate logical access rights and controls;
- Data encryption in accordance with <ORGANIZATION>'s encryption policies and standards defining algorithms, key lengths, key management and escrow *etc.*
- Accounting/audit logging of access checks, plus alarms/alerts for attempted access violations where applicable.

5.5.3 Procedural components of access controls shall be documented within procedures, guidelines and related documents and incorporated into awareness, training and educational activities. This includes:

- Choice of strong passwords;
- Determining and configuring appropriate logical access rights;
- Reviewing and if necessary revising access controls to maintain compliance with requirements;

5.5.4 Physical access controls shall include:

- Layered controls covering perimeter and internal barriers;
- Strongly-constructed facilities;
- Suitable locks with key management procedures;
- Access logging though the use of automated key cards, visitor registers *etc.*;
- Intruder alarms/alerts and response procedures;

5.5.5 If parts of <ORGANIZATION>'s IT infrastructure are to be hosted at a third party data centre, the data centre operator shall ensure that <ORGANIZATION>'s assets are both physically and logically isolated from other systems.

Outsourcing security policy

5.5.6 <ORGANIZATION> shall ensure that all information assets handed over to the outsourcer during the course of the contract (plus any copies made thereafter, including backups and archives) are duly retrieved or destroyed at the appropriate point on or before termination of the contract. In the case of highly classified information assets, this normally requires the use of a schedule or register and a process whereby the outsourcer formally accepts accountability for the assets at the point of hand-over.

5.6 Security audits

5.6.1 If <ORGANIZATION> has outsourced a business function to an outsourcer based at a different location, it shall audit the outsourcer's physical premises periodically for compliance to <ORGANIZATION>'s security policies, ensuring that it meets the requirements defined in the contract.

5.6.2 The audit shall also take into consideration the service levels agreed in the contract, determining whether they have been met consistently and reviewing the controls necessary to correct any discrepancies.

5.6.3 The frequency of audit shall be determined by management on advice from functions such as Internal Audit, Information Security Management and Legal.

6 Responsibilities

6.1 Management

6.1.1 Management is responsible for designating suitable owners of business processes that are outsourced, overseeing the outsourcing activities and ensuring that this policy is followed.

6.1.2 Management is responsible for mandating commercial or security controls to manage the risks arising from outsourcing.

6.2 Outsourced business process owners

6.2.1 Designated owners of outsourced business processes are responsible for assessing and managing the commercial and security risks associated with outsourcing, working in conjunction with Information Security, Legal and other functions as necessary.

6.3 Information Security

- 6.3.1 Information Security, in conjunction with functions such as Legal, Compliance and Risk Management, is responsible for assisting outsourced business process owners to analyze the associated risks and develop appropriate process, technical, physical and legal controls.
- 6.3.2 Information Security is also responsible for maintaining this policy.

6.4 Internal Audit

- 6.4.1 Internal Audit is authorized by management to assess compliance with all corporate policies at any time.
- 6.4.2 Internal Audit may assist with audits of outsourcing contracts including security compliance audits, and advise management on the risks and controls relating to outsourcing.

7 Copyright



This work is copyright © 2008, ISO27k Implementers' Forum, some rights reserved. It is licensed under the [Creative Commons Attribution-Noncommercial-Share Alike 3.0 License](https://creativecommons.org/licenses/by-nc-sa/3.0/). You are welcome to reproduce, circulate, use and create derivative works from this *provided* that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k Implementers' Forum (www.ISO27001security.com), and (c) derivative works are shared under the same terms as this.

8 Disclaimer

This is a generic example policy. It is not intended to suit all organizations and circumstances. It is merely guidance. Please refer to the ISO/IEC 27000-series standards and other definitive sources including qualified legal counsel in preparing your own security policies.