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.

Index

1 Introduction 3
2 Objective 3
3 Scope 3
4 Policy axioms 3
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 of employees 6
5.5 Access controls 7
5.6 Security audits 8
6 Responsibilities 8
6.1 Management 8
6.2 Outsourced business process owners 8
6.3 Information Security 9
6.4 Internal Audit 9
Copyright 9
Disclaimer 9

Version	Issued	Prepared by	Approved by	Description
1	2008	Aaron d'Souza and Gary Hinson		Generic policy template for www.ISO27001security.com
2	2022	Gary Hinson		Updated, 14 years down the line
3	2023	Gary Hinson		Minor tweaks, nothing substantial

1 Introduction

1.1.1 Outsourcing involves commercial arrangements to transfer responsibility for various business activities to third parties. Outsourcers provide services to <ORGANISATION> to a mutually agreed service level defined formally in a contract.

1.1.2 The providers of outsource services (outsourcers) are primarily business process and professional services specialists (*e.g.* IT, finance and HR services, consultants, telecommunications and networking services, cloud computing services), but may also include temporary staff and contractors or sub-contractors.

1.1.3 Many commercial benefits have been ascribed to outsourcing such as:

- Reducing the organisation's costs (assuming the outsourcer can perform the services more efficiently and does not over-charge);
- Greater focus on core business by outsourcing non-core functions;
- Access to additional specialist skills and resources.

1.1.4 Despite the potential benefits, information security incidents such as inappropriate access to or disclosure of sensitive information, loss of intellectual property or the inability of the outsourcer to meet agreed service levels, would reduce the benefits and could jeopardize the customer's information security.

2 Objective

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

3 Scope

The policy applies throughout <ORGANISATION>.

4 Policy axioms

4.1.1 The commercial benefits of outsourcing non-core business functions must be sufficient to offset the associated risks.

4.1.2 The risks associated with outsourcing must be mitigated to acceptable levels using appropriate administrative, physical and technical controls.

5 Policy statements

5.1 Choosing an outsourcer

5.1.1 Criteria for selecting an outsourcer include 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 conformity 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 should nominate a suitable <ORGANISATION> owner for each business function/process outsourced. The owner, with help from Information Risk and Security Management, should identify, evaluate and decide how to treat the information risks before the function/process is outsourced, using <ORGANISATION>'s risk management process.

5.2.2 In relation to outsourcing, specifically, the risk assessment should take due account of the:

- Nature of logical and physical access to <ORGANISATION> information assets and facilities required by the outsourcer to fulfil the contract;
- Sensitivity, volume and value of any information assets involved;
- Commercial risks such as the possibility of the outsourcer's business failing completely, failing to meet agreed service levels, or providing services to <ORGANISATION>'s competitors where this might create conflicts of interest; *and*
- Security and commercial controls known to be currently employed by <ORGANISATION> and/or by the outsourcer.

5.2.3 If the risks involved are considerable and the commercial benefits are marginal (*e.g*. if the controls necessary to mitigate the risks are too costly), a function or process should not be outsourced.

5.3 Contracts and confidentiality agreements

5.3.1 A binding contract is required between <ORGANISATION> and the outsourcer to protect both parties.

5.3.2 The contract should clearly define the types of information exchanged and the purposes for so doing. If the information being exchanged is sensitive, the outsource contract should contain suitable confidentiality clauses or a separate non-disclosure agreement should be in place (quite likely before the outsourcing contract is executed).

5.3.3 Exchanged information shall be classified and controlled in according with <ORGANISATION> policy, as a minimum.

5.3.4 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.

5.3.5 Draft contracts should be reviewed/updated and approved by Legal/Compliance before execution.

5.3.6 In addition to the commercial and legal formalities applicable any contract (*e.g*. the full names of the parties, charges and payment terms, jurisdiction), outsourcing contracts should clearly specify each party's responsibilities toward the other (*e.g*. service levels and penalties or liabilities for non-performance).

5.3.7 According to the information risk assessment, specific information security controls may be required, such as:

- Legal, regulatory and contractual compliance obligations such as data protection/privacy laws, money laundering, tax *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 prompt event and incident reporting (where 'prompt' means 'at the earliest practical opportunity' and 'event' includes early indications of possible security compromises and incidents ahead);

* In the case of "offshore" outsourcing, special consideration must be given to the ramifications of transferring information between countries or jurisdictions, particularly where privacy or other laws may conflict.

- 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, network and system security monitoring, logging 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;

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

5.3.8 Although outsourcers that are certified against ISO/IEC 27001 *may* have an effective Information Security Management System in place (depending on the scope and nature of certification), <ORGANISATION> may require additional assurance that important information security controls adequately address <ORGANISATION>'s specific requirements, potentially both prior to and during the outsourcing (see section 5.6).

5.4 Hiring and training of employees

5.4.1 Outsource employees, contractors and consultants working on behalf of <ORGANISATION> should be subjected to background checks equivalent to those performed on <ORGANISATION> 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 or similar official photo ID);
- Proof of their academic and professional 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 <ORGANISATION> or to outsourcers used by <ORGANISATION> shall perform at least the same standard of background checks as those indicated above.

5.4.3 Regardless of who formally employs them, appropriate information security awareness and training is required for all workers, clarifying their responsibilities relating to <ORGANISATION> 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 <ORGANISATION>'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 typically 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 <ORGANISATION>'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 and multi-factor authentication (especially for privileged accounts);
- 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 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 <ORGANISATION>'s IT infrastructure are to be hosted at a commercial data centre, <ORGANISATION>'s assets must be both physically and logically isolated from other systems and customers.

5.5.6 <ORGANISATION> 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 protecting the assets at the point of hand-over.

5.6 Security audits

5.6.1 If <ORGANISATION> 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 <ORGANISATION>'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

Management is responsible for:

- Designating suitable owners of business processes that are outsourced;
- Overseeing the outsourcing activities, ensuring that this policy and other applicable policies and procedures are followed;
- Mandating various controls to mitigate unacceptable risks relating to outsourcing.

6.2 Outsourced business process owners

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 Risk and Security Management

Information Risk and Security Management, in conjunction with functions such as Legal/Compliance, Risk Management and Procurement, is responsible for:

- Assisting outsourced business process owners to identify and evaluate the associated information risks, and select appropriate controls;
- Assisting with the design, implementation, monitoring and management of the controls;
- Maintaining this policy.

6.4 Internal Audit

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