Outsourcing Policy

Objective

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

Scope

The policy applies throughout Novus Altair

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

The policy addresses the following controls found in the ISO/IEC 27002 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

Policy statements

Choosing an outsourcer

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 90001 and ISO/IEC 27001, ISO 14001 & ISO 45001).

Further information security criteria may be defined as the result of the risk assessment (see next section).

Assessing outsourcing risks

Management shall nominate a suitable company for each business function/process outsourced. The MD, shall assess the risks before the function/process is outsourced, using Pentest People's standard risk assessment processes.

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

a) nature of logical and physical access to Companies 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 Novus Altair's competitors where this might create conflicts of interest; *and*

d) security and commercial controls known to be currently employed by Novus Altair and/or by the outsourcer.

The result of the risk assessment shall be presented to management for approval prior to signing the outsourcing contract. Management shall decide if the Company 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.

Contracts and confidentiality agreements

A formal contract between Novus Altair 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.

If the information being exchanged is sensitive, a binding confidentiality agreement shall be in place between Novus Altair 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).

Information shall be classified and controlled in according with Novus Altair's policy.

Any information received by Novus Altair from the outsourcer which is bound by the contract or confidentiality agreement shall be protected by appropriate classification and labeling.

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.

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

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.
- 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*.
- 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;

- The right of the Company to monitor all access to and use of Novus Altair's 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.

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 Novus Altair to verify security controls that are essential to address the companies' specific security requirements, typically by auditing them

Hiring and training of employees

Outsource employees, contractors and consultants working on behalf of Novus Altair shall be subjected to background checks equivalent to those performed on Novus Altair 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.

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

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 Novus Altair's 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.

Access controls

In order to prevent unauthorized access to Novus Altair'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.

Technical access controls shall include:

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

Procedural components of access controls shall be documented within procedures, guidelines and related documents and incorporated into awareness training 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;

Physical access controls shall include:

- A well constructed facility;
- Suitable locks with key management procedures;
- Intruder alarms and response procedures;

Novus Altair 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.

Security audits

If Novus Altair 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 Novus Altair's security policies, ensuring that it meets the requirements defined in the contract.

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.

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

Responsibilities

Management

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

The Directors are responsible for mandating commercial or security controls to manage the risks arising from outsourcing.

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.

Signed Dr Adnan Niazi

Date 4/1/2021

Last Reviewed On 05/07/24

Version 1