

Externally provided processes, products and services Policy

Objective

This policy specifies controls to reduce the information security, reputation and quality risks associated with externally provided processes, products and services.

The policy applies throughout Interr Ltd:

Externally provided processes, products and services include:

- hardware and software support and maintenance staff
- external consultants and contractors
- IT or business process outsourcing firms
- temporary staff

Policy statements

Choosing externally provided processes, products and services

Criteria for selecting an externally provided processes, products and services 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;
- assurances of fair treatment of all staff and contractors and social corporate responsibilities;
- quality assurance and security management standards currently followed by the company (e.g., certified compliance with ISO 9001, 14001, 45001, SIA ACS and ISO/IEC 27001);
- commitment to supplier's diversity initiatives and preference will be given to suppliers who are registered/certified diverse-owned or small businesses (DOSB);
- alignment with Interr's Policies, contractual and legal requirements.

Externally provided processes, products and services are subject to the same management disciplines that would apply as if the service was not outsourced. It is important for us to recognise that externally provided processes, products and services and business activity does not transfer all the risks associated with that activity to the external providers. Appropriate due diligence as outlined below must be used when considering the outsourcing of an activity and selecting third party service providers/ externally provided processes, products and services.

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

Assessing externally provided processes, products and services risks

Management shall nominate a suitable company for each externally provided processes, products and services. The Executive led by the CEO, shall assess the risks before the function/process is outsourced, using Interr Security's standard risk assessment processes.

In relation to externally provided processes, products and services, specifically, the risk assessment shall take due account of the:

- nature of logical and physical access to Companies information assets and facilities required by the externally provided processes, products and services to fulfil the contract;
- sensitivity, volume and value of any information assets involved;
- commercial risks such as the possibility of the externally provided processes, products and services business failing completely, or of them failing to meet agreed service levels or providing services to Interr Security's competitors where this might create conflicts of interest; and

- security and commercial controls known to be currently employed by Interr Ltd and/or by the externally provided processes, products and services.
- Confirmation of company policies and procedures, including but not limited to environmental, H&S, D&I, Anti-corruption and bribery, Business Continuity, Data Protection and Info Sec.
- Levels of insurance
- Legal registrations and compliance
- International Sanctions and Watch Lists

The risk assessment/due diligence result shall be presented to management for approval before signing the externally provided processes, products and services contract. Management shall decide if the Company will benefit overall by outsourcing the function to the externally provided processes, products and services, 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 Interr and the externally provided processes, products and services 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 Interr and the externally provided processes, products and services, 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 accordance with Interr Security's policy.

Any information received by Interr from the externally provided processes, products and services which is bound by the contract or confidentiality agreement shall be protected by appropriate classification and labelling.

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 Executive and or 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 externally provided processes, products and services after the completion of the externally provided processes, products and services' activity or whenever the asset is no longer required to support the externally provided processes, products and services activity;
 - Copyright, patents and similar protection for any intellectual property shared with the externally provided processes, products and services 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, anti virus 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 Interr Security's facilities, networks, systems etc., and to audit the externally provided processes, products and services' 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 externally provided processes, products and services 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 Interr Ltd to verify security controls that are essential to address the companies' specific security requirements, typically by auditing them.

Physical media in transit

Media/equipment will whenever possible be transported by Interr staff, and when that is not doable by reliable authorized couriers only (royal mail special delivery) and the equipment/media protected so as to ensure the information is not accessible. Also, all such transportation must be authorized by a HOD each time it needs to happen.

Packaging should be sufficient to protect the contents from any physical damage during transit and should be in accordance with manufacturers' specifications or in accordance with the level of security classification. Also, all such transportation must be authorized by a HOD each time it needs to happen.

Special measures will be adopted, where necessary, to protect sensitive information from unauthorised disclosure or modification. Sending paper confidential information should only happen when it is essential to do so and there is no alternative method for accessing or recording the information required.

Where paper records must be taken off site, only the minimum amount of personal or other confidential data necessary for the job in hand should be removed. Where possible, data should be anonymised.

This should also include:

- use of locked containers;
- delivery by hand by a designated staff member;
- tamper-evident packaging (which reveals any attempt to gain access);
- in exceptional cases, splitting of the consignment into more than one delivery and dispatch by different routes.

Hiring and training of employees

Externally provided processes, products and services employees, contractors and consultants working on behalf of Interr Security shall be subjected to background checks equivalent to those performed on Interr Security 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 Interr or to externally provided processes, products and services used by Interr 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 Interr Security 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 Interr's information assets by the externally provided processes, products and services 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 Interr Security'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;
- Interr Ltd shall ensure that all information assets handed over to the externally provided processes, products and services 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 Interr has outsourced a business function to an externally provided process, products and services based at a different location, it shall, when required, audit the externally provided processes, products and services's physical premises periodically for compliance to Interr'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 outsourced business processes, overseeing the externally provided processes, products and services and activities and ensuring that this policy is followed.

The Directors are responsible for mandating commercial or security controls to manage the risks arising from externally provided processes, products and services.

Externally provided processes, products and services business process owners

Designated owners of externally provided processes, products and services and 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.

Policy Review and Assessment

This policy may be amended by Interr at any time in order to take into account changes in legislation and best practice. This policy was last reviewed and agreed by the Board and seeks to be reviewed and updated annually. Any queries arising regarding this policy should be addressed to Mick Tabori.



Mick Tabori - CEO
July 2024