Information Security and Confidentiality Compliance Requirements

Version 6 – 31/01/2024

Sede legale:
Via San Gregorio 34
20124 Milano
t +39 02 22190111
f +39 02 22190100

Capitale Sociale € 2.522.319 i.v.
P.IVA 13251500156
C.F. 06602910017

Sede amministrativa:
Via Cesare Pavese 6
10015 Ivrea, TO
t +39 0125 935111
f +39 0125 935100

info@rgigroup.com
www.rgigroup.com

Contents

Sede legale:
Via San Gregorio 34
20124 Milano
t +39 02 22190111
f +39 02 22190100

Capitale Sociale € 2.522.319 i.v.
P.IVA 13251500156
C.F. 06602910017

Sede amministrativa:
Via Cesare Pavese 6
10015 Ivrea, TO
t +39 0125 935111
f +39 0125 935100

info@rgigroup.com
www.rgigroup.com

Sede legale:
Via San Gregorio 34
20124 Milano
t +39 02 22190111
f +39 02 22190100

Capitale Sociale € 2.522.319 i.v.
P.IVA 13251500156
C.F. 06602910017

Sede amministrativa:
Via Cesare Pavese 6
10015 Ivrea, TO
t +39 0125 935111
f +39 0125 935100

info@rgigroup.com
www.rgigroup.com

Information Security and Confidentiality Compliance Requirements

1. Introduction

1.1. Scope of application of this document

The aim of the document is to define the guidelines and organizational-technical-administrative requirements to ensure that adequate levels of security are met within the procedures for the procurement of IT goods and services for RGI Spa.

During the acquisition processes, it is believed that, due to the nature of the services offered, suppliers may have access to RGI Spa's information assets, thereby introducing potential information risks, with an impact on data confidentiality, integrity, availability, authenticity and non-repudiation.

Acquisition processes conducted without attention to information security may render ineffective, or in any case less effective, the measures taken by RGI Spa to protect its information assets.

As such, this document has a limited scope and concentrates on security in the procurement of information products and services, while also covering the broad topic of information security.

It is useful, in this Introduction, to point out that the contracts concluded by RGI Spa with suppliers concerning ICT:

- may result from a bid or represent specific framework agreement contracts;
- may be multi-annual (some degree of turnover of supplier personnel is therefore inevitable);
- may include more than one project initiative, typically several distinct projects conducted partially sequentially, partially concurrently, and not necessarily by the same supplier team;

For the purposes of this document, ICT contracts can be classified as follows:

- contracts for the development, implementation and maintenance of computer applications;
- hardware or software product procurement contracts;
- operations and management contracts;
- contracts for services other than a) and c) (e.g. support, consultancy, training, help desk, and so forth);
- contracts for a combination of the above categories of supplies.

Sede legale:
Via San Gregorio 34
20124 Milano
t +39 02 22190111
f +39 02 22190100

Capitale Sociale € 2.522.319 i.v.
P.IVA 13251500156
C.F. 06602910017

Sede amministrativa:
Via Cesare Pavese 6
10015 Ivrea, TO
t +39 0125 935111
f +39 0125 935100

info@rgigroup.com
www.rgigroup.com

1.2. Target group for the document

The document's contents are to be interpreted in terms of guidelines and procedures with which the supplier must comply, taking into account the relevance and criticality profiles of the various ICT acquisitions to be conducted, as detailed for each indication in Chapter 2.

The document is targeted at RGI Spa's suppliers, who should be aware of information security issues to be prepared to satisfy the customer's requirements without a significant impact on negotiations and in a spirit of cooperation.
It is deemed necessary to establish a common vocabulary and to share security objectives to benefit not only RGI Spa but also suppliers by improving the efficiency of contract clauses.

1.3. Aims of this document

The aims of this document are to:

- exemplify information security issues in a straightforward and immediately applicable manner;
- put the document in the system (using appropriate glossaries and categorizations) definitions and concepts pertaining to information security and formalize and make them consistent with the standard and the context of RGI Spa's operational activities;
- provide security measures to be adopted by the supplier (operational tools, practical examples, specific references) to ensure that the activities provided adhere to the level of security of the current processes at RGI Spa, and possibly propose solutions to raise this level without excessively increasing the complexity and effort required to conduct the processes.

1.4. Definitions

- **Framework Agreement** - an agreement that establishes the general terms (e.g. unit fees, Service Level Agreements, etc.) regulating the contracts to be signed within a given time frame. RGI Spa then negotiates individual contracts tailored to its requirements (quantities, specific characteristics, etc.) within the context of the Framework Agreement.
- **Account Management** - Management of accounts and credentials.
- **Asset Management** - Management of assets covered under the service/supply contract.
- **Audit** - Independent process of assessment and control.

- **Change Management** - A strategy for managing the transition or transformation of an organization's objectives.
- **Code Review** - The process of reviewing code and programming instructions.
- **Penetration Test** - The process of assessing the security of a system or network by simulating a cyberattack.
- **Risk Management** - The process of identifying, evaluating and dealing with threats to an organization's assets and earnings.
- **Vulnerability Assessment** - The process of identifying and classifying a system or network's security flaws.
- **Web Server** - Software application installed on a server that handles web page requests from client web browsers.
- **Wiping** - The process of permanently erasing data contained on a storage medium, e.g. a hard disk.

1.5. Personal data

Identification Data - Information that can directly or indirectly identify a person, including their name, identification number, location data or online identifier.

Particular Data - Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, as well as genetic data, biometric data intended to uniquely identify a living individual, health or reproductive life or sexual orientation data. (pursuant to Art. 9 of the Regulation).

Judicial Data - Data concerning criminal convictions and offences or related security measures (pursuant to Art. 10 of the Regulation).

2. Security Requirements - Rules of Conduct

2.1. Information Management - General

Without prejudice to the provisions of the Terms and Conditions, in each Contract and other Annexes relating to Privacy and Confidentiality, the Supplier shall, in performing each service for the benefit of RGI Spa, comply with the following management rules:

- The Supplier formally acknowledges its responsibility for the protection of confidential information by signing a confidentiality undertaking and a non-disclosure agreement (NDA);
- All information sent by RGI Spa to the Supplier or accessible to the Supplier through agreed-upon means remains the property of RGI Spa and to any third parties who have entrusted it to RGI Spa. Therefore, any such information must not be:
  - used by the Supplier, except within the scope of the Contract;
  - disclosed, sold or transferred;
  - provided to third parties, except in cases covered under the Contract;
  - commercially exploited by or on behalf of the Supplier.
- Upon termination of the work, Contract, or Agreement, the Supplier is required to promptly return all assets, including data, owned by RGI Spa and third parties. In addition, the Supplier must provide proof that it has erased all information, data and assets received from or produced for RGI Spa during the term of the Contract;
- During all stages of information processing, the Supplier must ensure that the data classification specified by RGI Spa (in terms of confidentiality, integrity, and availability) is adhered to;
- The Supplier (and any person employed or instructed by it in connection with the service offered) must ensure that its use of RGI Spa's confidential information is limited to the performance of services under the terms of the Agreement;
- The Supplier undertakes to comply with the security measures implemented by RGI Spa for the protection and use of the data. In the event of data migration, the Supplier undertakes to draw up an alternative plan and a recovery plan to prevent the loss or corruption of RGI Spa's information. The substitute plan must be submitted to RGI Spa for approval.

Sede legale:
Via San Gregorio 34
20124 Milano
t +39 02 22190111
f +39 02 22190100

Capitale Sociale € 2.522.319 i.v.
P.IVA 13251500156
C.F. 06602910017

Sede amministrativa:
Via Cesare Pavese 6
10015 Ivrea, TO
t +39 0125 935111
f +39 0125 935100

info@rgigroup.com
www.rgigroup.com

2.2. Information Management - Confidentiality, Integrity, Availability

The Supplier shall observe the following rules of conduct in the performance of each service or contract:

- adopt protective measures to ensure the confidentiality of RGI Spa's proprietary information and third-party information entrusted to RGI Spa, whether stored or in transit, which may include an appropriate logical access control policy and/or procedure that, among other things, provides for:
  - implement policies for managing records of information events (at least administrative access records - normal access records);
  - comply with the requirements concerning the encryption of confidential and secret information laid down in the RGI Spa data classification policy;
  - comply with the requirements concerning the encryption of communications;
  - comply with key management requirements;
  - grant access to RGI Spa's information to its personnel using the “need to know” principle and minimum privilege.
  - If the Supplier must use sub-suppliers or sub-contractors, it shall take all precautions necessary to protect RGI Spa's confidential information and assets. The appointment of sub-suppliers and sub-contractors shall be notified to RGI Spa, which reserves the right to accept or reject the appointments, communicating its decision in writing.
- demonstrate that an appropriate “Clear Desk and Clear Screen” policy has been adopted. This policy must be implemented obligatorily for all activities involving the information of RGI Spa and that of third parties.
- provide that all paper documents or other media containing information of RGI Spa and/or third parties is stored under lock and key in cabinets or in suitable filing cabinets protected by a numerical combination lock when not being used for activities related to the contracted services;
- not make copies of documents classified by RGI Spa, or by third parties, as “**Secret**” and “'**Confidential**” without the prior authorization of the owner of the information;
- not make copies of documents classified by RGI Spa, or by third parties, with the "**Reserved**" level using shared printers outside strictly controlled areas;
- use devices for the printing and/or large-scale export of confidential information that requires specific authorization from RGI Spa Moreover, the printing or export process must be adequately monitored.

Sede legale:
Via San Gregorio 34
20124 Milano
t +39 02 22190111
f +39 02 22190100

Capitale Sociale € 2.522.319 i.v.
P.IVA 13251500156
C.F. 06602910017

Sede amministrativa:
Via Cesare Pavese 6
10015 Ivrea, TO
t +39 0125 935111
f +39 0125 935100

info@rgigroup.com
www.rgigroup.com

2.3. Information Management - Risk Management

2.3.1. Information Risk Management Policies

The Supplier must demonstrate that it has a risk management policy covering at least the following areas:

- assessment and treatment of risks related to logical access controls with particular reference to:
  - the on-boarding process
  - the out-boarding process
  - the role/skill change management process
  - the periodic verification of user access rights
- the assessment and treatment of risks related to the management of the roles and responsibilities assigned to each party
- the risk assessment and treatment of information concerning:
  - processes related to confidentiality
  - processes related to integrity
  - processes related to availability
- the assessment and treatment of security risks in the areas where information is processed
- the assessment and treatment of IT infrastructure security risks with regard to redundancy of network equipment, systems and devices
- the assessment and treatment of process-related risks relating to the roles and responsibilities of users handling and managing RGI Spa information in whatever context
- the risk assessment and treatment related to the process of training users on information security, data security in general and awareness of related risks (including cyber security related risks);
- the assessment and treatment of security risks in the development of systems and their maintenance;
- the assessment and treatment of risks related to compliance with applicable regulations;
- the assessment and treatment of IT supply-chain security risks
- the assessment and treatment of supplier-related security risks
- Data Leakage and Data Loss Prevention risk assessment and treatment

The Supplier shall appoint a person responsible for the management of the above-mentioned risks. Said appointee shall be responsible for the protection of RGI Spa's proprietary information and any information that third parties have entrusted to RGI Spa

Periodically, the Supplier shall evaluate the risks influencing the contract activities with RGI Spa, approving the results and proposed action plans. The Supplier shall also notify RGI Spa of any changes to the agreed-upon dates for the performance of specific risk management tests and comply with the agreed-upon procedures for controlling any delays

The Supplier must demonstrate that it has activated the process related to the disclosure of its responsibilities with regard to:

- maintaining knowledge of and compliance with published security policies, procedures, standards and applicable regulatory requirements;
- maintaining a safe and secure working environment; protecting unmanned devices.
- inform RGI Spa of any changes in the business environment that could have a significant effect on the level of security of the service;

2.3.2. Risk Monitoring

The Supplier must establish risk monitoring procedures for personnel management, ensuring in particular that:

- all Supplier personnel and subcontractors shall be required to sign a confidentiality agreement for information owned by RGI Spa and entrusted to RGI SpaRGI Spa by third parties;
- the proposed Information Risk Management programme shall also take environmental risks into account;
- the Supplier shall put into place an appropriate procedure for the resolution of disputes concerning activities falling within the scope of information risk management.
- monitoring and reporting on cyber risk management shall be implemented as a minimum by:
    - surveillance and security status notification;
    - notification of any incidents relating to IT risk management;

2.4. Managing disclosure and awareness constraints

The supplier must demonstrate that it has set up an awareness programme for its personnel (employees, third parties, etc.) on issues related to information disclosure constraints, following the guidelines below:

- - dissemination and adoption of the relevant guidelines and information management policies, with an absolute prohibition on:

- making information managed by the Company available outside its organizational structure (e.g. if an employee changes company) without the express authorization of the Information Manager;
- excessive or indecent use of the Internet;
- accessing or exchanging defamatory messages, consulting websites that incite hatred or gambling;
- accessing illegal information, e.g. copying copyrighted information such as images, sounds or software from the Internet;
- automatic sending of internal e-mails via the Internet to private or unauthorized accounts.

- Collaborators must be aware of:
  - risks and precautions when downloading files or code from the Internet;
  - risks and precautions against downloading malware from the Internet;
  - proper use of removable storage devices.
  - phishing risks
  - risks related to social engineering techniques
- individual responsibility is an essential aspect of information security and must be achieved through a combination of high standards of conduct, audits and controls in accordance with the spirit of the security regulations:
  - each employee (including temporary staff) must protect information security resources, in particular computing devices during their movement and use at remote sites or when working remotely;
  - each employee (including temporary staff) must report information security incidents to the Information Security Office according to the procedures;
  - users must not interfere with the operations performed by the security platforms. Users must not try to circumvent security controls;
  - users must comply with software licence requirements and copyright restrictions;
  - users must be informed of the dangers caused by computer viruses and of best practices to reduce the chances of infection. Users must use antivirus software and take appropriate measures with regard to the risk caused by computer viruses;
  - If a user detects a virus, must immediately follow corporate procedures;
  - employees of Suppliers (including temporary staff) shall not take any action that may prevent and/or restrict the management functions for reviewing messages and transactions (e.g. use of personal encryption software);
  - employees of Suppliers (including temporary staff) must comply with the Company's standards and those that may be imposed by RGI Spa.
  - employees of Suppliers (including temporary staff) must not establish connections, install electronic devices and/or use personal software;

- employees of Suppliers (including temporary staff) must protect their credentials, passwords and the system for managing and generating authorization tokens (MFA);
- employees of Suppliers (including temporary staff) must comply with applicable laws and regulations.
- The programme to raise employee awareness must cover information and data security and cyber risks

- In the process of selecting and orientating office staff, consultants and third party companies, the Supplier shall adhere to at least the following security-related evaluation criteria:
  - new employees, including temporary staff and external consultants, must accept and sign a security information document. No right of access may be granted before this document has been signed;
  - information provided by candidates (identity, certificates, etc.) must be verified by HR staff who have access to sensitive resources (software or data).
- The Supplier's risk manager must ensure that staff understand the threats related to the department and its Information Management policies;
- Supplier personnel assigned to perform a service must receive regular training and updates on policies and procedures relevant to information risk management and must be informed about RGI Spa's system for risk classification and the appropriate procedures communicated by the latter;
- The Supplier's subcontractors appointed to perform the service must be informed of RGI Spa's risk classification system and of the appropriate procedures communicated by the latter.

Sede legale:
Via San Gregorio 34
20124 Milano
t +39 02 22190111
f +39 02 22190100

Capitale Sociale € 2.522.319 i.v.
P.IVA 13251500156
C.F. 06602910017

Sede amministrativa:
Via Cesare Pavese 6
10015 Ivrea, TO
t +39 0125 935111
f +39 0125 935100

info@rgigroup.com
www.rgigroup.com

2.5. Safe development activities

The Supplier must have security policies in place that explicitly state the security requirements and processes to be adopted during the development of software and applications, designed according to accepted commercial security standards (e.g. OWASP for web applications) and compliant with regulations.

2.5.1. Functional security requirements

Functional security requirements concern the functions usually visible to users of a software programme. The Supplier must be able to prove that these requirements have been documented in functional specification documents. A list of common requirements to be adopted by the Supplier now follows:

- the methods of user authentication in the development environments, which could be based on passwords, tokens or biometric characteristics or combinations thereof; the functional requirements must also specify how to ensure the security of the authentication mechanism (password characteristics, masking of the password on the login page, credential control only on the server, encryption of communication); the use of an external authentication mechanism or MFA techniques may also be envisaged;
- provide for the profiles, roles and authorisations required by the software, including any separation of duties;
- provide for the limitation of functionalities and queries to users on the basis of their profile;
- provide for administration utilities and their authorisations;
- provide for ways of interfacing with other software; this should take place over encrypted channels set up with the exchange of certificates so as to guarantee the identification of the different instances;
- provide for transmission modes over the Internet based only on encrypted channels;
- prevent the ability of users to access data directly without the mediation of the application;
- provide for referential integrity choices in databases;
- provide for choices concerning competing transactions in the databases (e.g. if a transaction is competing with one already started, the user must be notified so that he or she can decide whether to submit it again);
- methods for checking the integrity of transactions (e.g. through control characters, unintended duplicate detection, ACK to user);
- methods for confirming user actions where appropriate (e.g. with confirmation messages when data are to be deleted);
- logging of activities whose logs are protected with anti-tampering tools and for which an appropriate retention time has been decided;

Sede legale:
Via San Gregorio 34
20124 Milano
t +39 02 22190111
f +39 02 22190100

Capitale Sociale € 2.522.319 i.v.
P.IVA 13251500156
C.F. 06602910017

Sede amministrativa:
Via Cesare Pavese 6
10015 Ivrea, TO
t +39 0125 935111
f +39 0125 935100

info@rgigroup.com
www.rgigroup.com

- methods for managing planned capacities (e.g. maximum number of planned users) and the possibility of increasing them (scaling);
- misuse cases, i.e. potential user actions that could damage the application or lead to security problems;
- applicable laws, other regulations and contractual obligations and their applicable requirements (e.g. personal data processing regulations, banking regulations, customer requirements);
- options for configurating security mechanisms available to system administrators and users.

2.5.2. Technical security requirements

The technical security requirements are divided into two families:

- refining functional requirements, and
- architecture-related requirements.

The Supplier must document its requirements within specifications or, when following Agile methods, in “definitions of done” or in tasks linked to user stories.

For the technical requirements to refine the functional ones, the supplier must demonstrate that it uses one or more of the following:

- credential caching modes;
- control and sanitization of input data from users and other processes;
- control of user queries;
- choice of cryptographic protocols and their settings (e.g. for key length).

For architectural requirements, the Supplier must demonstrate that it uses one or more of the following:

- division into several levels or tiers (e.g. database, application, presentation);
- cohesion of modules (each module must serve a unique purpose);
- separation of access control and authorizations from other modules;
- separation of the administration interface from the other modules;
- decoupling of modules (loose coupling), which includes the prohibition of encoding data, configurations and passwords in software objects;
- verification of authorizations for each operation on an object or data (full mediation);

- users and their authorizations for interfacing with other systems;
- secure management of sessions and their parameters;
- choice of externally sourced software and libraries (for which source reliability and maintenance availability must be ensured);
- configuration management to enable timely patching and fixing;
- management of operations when one of them gives an error; in particular, all subsequent operations should be blocked and the user should be warned (fail safe);
- interception of all possible errors, so that they can be handled.

2.5.3. Coding requirements

The Supplier must also demonstrate that it uses these requirements by providing evidence of their publication in specific documents (including in wikis for internal use or in Safe Development Rules) or, when following Agile methods, in “definitions of done”.

The coding rules to be followed depend on the language used; therefore, the Supplier will only be required to demonstrate what is valid in its own development field by including one or more of the following requisites:

- define a standard for naming classes, methods, variables and constants so that their purpose and nature can be understood;
- the management of comments (quantity, placement, care that they do not contain information that can be used for understanding the system architecture or other critical information);
- management of variables to prevent the most common attacks;
- the list of functions to be avoided.

2.5.4. Test verification and release

The Supplier must carry out a final verification of the security status of the developed software (including penetration tests) as part of the release process to ensure that there are no known vulnerabilities. In addition, the Supplier must guarantee at least the following:

- support the execution of vulnerability and penetration tests performed by RGI Spa (or delegated personnel/third parties) for the purpose of verifying the security of software and systems;
- undertake to implement action plans to correct any vulnerabilities, agreeing timeframes and methods with RGI Spa, based on the Group's standards, which generally provide 30 days to

resolve "Critical" vulnerabilities, 45 days for "high" vulnerabilities, 90 days for "medium" vulnerabilities and 180 days for "low" vulnerabilities;
- perform or allow automatic or manual code review (source code review) to ensure that the code is free of security vulnerabilities.

2.6. Copyright management

The Supplier shall demonstrate a responsible attitude towards copyright that may relate to the use and licensing of the software, which includes:
- procedures for managing software licences;
- control and explicit prohibition of the use of unauthorized/unlicensed software;

2.7. Artificial Intelligence

The Supplier must declare its internal processes for the use of artificial intelligence with particular reference to the areas that may be included in the services contracted with RGI Spa.
Within the scope of the contract with RGI Spa, the Supplier must strictly prohibit the use of external platforms for artificial intelligence to avoid compromise and unauthorized disclosure of RGI Spa's code, data and information.

3. Incident Management

The Supplier must demonstrate that it has implemented an Incident Management process with sequenced operations for its resolution. In addition, the Supplier must demonstrate the methodology applied for recording incidents. Records must contain sufficient information for detailed analysis; incident and vulnerability tickets must be classified and prioritized appropriately according to severity, and defined escalation and communication procedures must be followed to ensure impact minimization and appropriate information to management. The Supplier must also demonstrate its incident resolution strategy. This strategy should provide for the appointment of incident collectors for each contracted service area. Managers should have the task of collection but also that of identifying and guiding activities and efforts related to incident resolution.

The Supplier must ensure that its Incident Management processes are properly managed at no additional cost to RGI Spa, in accordance with the deadlines defined in the service level agreement; in addition, the Supplier must:

- enable RGI Spa to detect and take action following information security incidents involving security incidents;
- ensure that activity logs on services provided are available for the proper handling of information security incidents;
- immediately inform the RGI Spa Contract Manager of any ascertained or suspected compromise; in the event of the compromise of privacy data, the Supplier shall comply with the constraints imposed by the applicable legislation on the protection of privacy by notifying RGI Spa within 24 hours of ascertaining the possible/probable compromise

3.1. Management process and resolution

In the event of a confirmed or suspected incident or vulnerability, security managers for the events under analysis are responsible for ensuring that the efforts required in their area of remit are properly understood, allocated and prioritized.
The relevant security officer will be involved in all 4 phases of the incident, i.e:

- **Detection** - This phase is to identify the mode of discovery by providing automatisms for the next phase where the incident is recorded by initiating the process. The Supplier must consider the progress of the management process by paying attention to time-tracking.
- **Analysis and classification** - The supplier shall classify the incident according to parameters such as type, initial impact assessment and urgency of management. The evaluation will provide the basis for the correct prioritization of the incident. This classification should be

preparatory to the correct choice of who should deal with the incident, the management methodology and the use of any workarounds, if they are present in the Knowledge Base.

- **Containment, Eradication and Restoration** - The Supplier must carefully follow this step, which can be assigned to a single person if the incident has been dealt with in the past and successful containment techniques or solutions have been used. In the event of a new type of incident, or in the event of a complex situation, the Supplier must have a management procedure with a cross-function team to manage the incident more effectively. The diagnosis may result in a new classification of the incident. **An incident will be resolved** when the mitigation solution is put in place automatically or the recovery procedure is provided to the user(s) or, finally, is managed by a dedicated team that will implement all the necessary activities. **Should the resolution times exceed any contractual SLAs**, the Supplier shall implement recovery strategies through the Disaster Recovery plans agreed with RGI Spa. In addition, the Supplier must prove that it has activated the process for the closure of incidents that includes:
  - the procedure for notifying stakeholders affected by the closure of the incident and the resumption of normal work activities;
  - a summary of all the incident management activities;
  - the procedure for reviewing, if necessary, the documentation of the configurations of the corporate assets subject to mitigation of the incident;
- **Post-incident activities** - The supplier must demonstrate that it has a post-analysis process that includes:
  - analysis of activities to identify those that brought positive effects and those that did not bring positive effects to the resolution of the incident
  - creation of an incident management playbook for inclusion in the knowledge base
  - periodic incident testing process to improve operational readiness

3.2. Incident Response Team (IRT)

The Supplier is also required to provide evidence of the organization of its own Incident Response Team (IRT) or, alternatively, to set up one for the management of incidents on information provided by RGI Spa. In addition, the Supplier's IRT shall be able to cooperate with the emergency response team identified by RGI Spa, in the event of a breach of serious risk management.

4. Logical controls and security measures

4.1. General security measures

The Supplier must ensure the implementation of adequate logical security controls to be applied to the data and environments covered by the contract in accordance with the following requirements of RGI Spa:

- The Supplier shall ensure that the necessary environment documentation (IT Infrastructure), e.g. user and administrator operating guides, diagrams of the contracted system architecture, any PlayBooks for the management of special areas, etc., are made available to authorized personnel in order to guarantee:
  - the design, installation and operation of the contract-related information system;
  - the effective use of the system's security functions.
- the Supplier shall also ensure the logical separation of RGI Spa's DATA from the data of other Customers, which in its Data Centre and all IT equipment, including Cloud environments, are used to provide services for RGI Spa;
- the RGI Spa environment, the subject matter of the contracted service, at the Supplier's premises or managed by it (Cloud) must be separated at least logically from the other infrastructures to ensure that it cannot be penetrated by the environments or networks of other customers of the Company;
- the separation of the development environments relating to the application components covered by the contracted services (presentation, data processing, database, identification and authentication process, etc.) is guaranteed and, if possible, hosted on different physical or virtual servers so that the various components are located in different areas on the network architecture.

Sede legale:
Via San Gregorio 34
20124 Milano
t +39 02 22190111
f +39 02 22190100

Capitale Sociale € 2.522.319 i.v.
P.IVA 13251500156
C.F. 06602910017

Sede amministrativa:
Via Cesare Pavese 6
10015 Ivrea, TO
t +39 0125 935111
f +39 0125 935100

info@rgigroup.com
www.rgigroup.com

4.2. Logical Access Control and encryption of information flows

The Supplier must accept the restrictions and security measures of RGI Spa set out below:

- RGI Spa grants minimum access for the proper management of the services relating to the Contract. If the Supplier requires access to certain applications, this must, where possible, be provided through a terminal services system. If this is not possible, common systems will have to be configured on a specific DMZ.
- The Supplier must ensure that it will manage access rights to operating systems and applications according to the principle of “Least Privilege”.
- The transfer of data between RGI Spa and the Supplier shall take place via a private, secure end-to-end connection using a level of encryption that guarantees the integrity of the connection and that is aligned with the most “robust” commercially available encryption standards.
- Wherever possible, the connection between the Supplier and RGI Spa shall use mechanisms enabling access and connections to be profiled exclusively to what is required for the service.
- In the event that a classical VPN connection is required, the encapsulation of the application (e.g. via terminal services) must be carried out using strict controls that allow access segmentation as specified above;
- workstations must have encrypted local storage media
- Removable storage media may only be used if they are duly protected by a media encryption system

4.3. End-point security

The workstations used by the Supplier's personnel must guarantee the following end-point security measures:

- Antimalware installed with daily updates managed remotely. Antimalware SW must include an advanced threat prevention solution that cannot be deactivated by the user
- Personal Firewall installed and active and which cannot be deactivated by the user
- Management of the WEB Filtering process to prevent browsing on sites not relevant to the activities
- adoption of data leakage prevention systems
- the Supplier must apply the necessary filtering systems to prevent unrestricted access from the internet to the administrative interfaces of the websites;
- blocking of data sharing on Cloud platforms not approved by RGI Spa
- The use of personal devices (BYOD) is not consented for the activities covered under the contracted services

- the Supplier shall not establish connections or install systems that allow end-point control (excluding suppliers responsible for network management), that may interfere with the control of an insurance company's network, and/or that allow the installation of backdoors;
- remote maintenance of end-points (including servers) must be described in a procedure. The procedure must provide for adequate security measures, control activities and recording of all maintenance operations performed remotely. Access to systems for remote maintenance must take place over a secure channel using appropriate cryptographic tools.
- The Supplier must ensure and demonstrate the inhibition of end-points to simultaneously connect to a network under the service contract to an insecure network (e.g. Wi-Fi connections).
- Policies and procedures should be established and implemented to limit access to sensitive data from mobile and portable devices, such as laptops, mobile phones and smartphones, which are generally more at risk than non-portable devices.

4.4. Secure Wiping. - Secure Disposal

SECURE WIPING - The Supplier must demonstrate that it has implemented a policy for the secure erasure of data on decommissioned or reassigned media. The policy must provide for increasingly stringent methodologies to ensure greater attention to wiping techniques for classified information. The wiping process must also provide for the secure collection of evidence of the deletion of data in order to be able to comply with any requests from RGI Spa. The procedure must provide for the complete recording of all wiping operations

SECURE DISPOSAL - The Supplier must demonstrate that it has implemented a secure disposal policy for all media, devices and systems that are to be decommissioned. Operational procedures must demonstrate the implementation of appropriate destruction measures, increasing in stringency according to the level of confidentiality of the equipment, device or system to be decommissioned. The procedure must provide for the complete recording of all wiping operations.

4.5. Secure Baseline

The Supplier must implement appropriate security configurations of devices, applications, equipment and systems, which take the following minimum requirements into account:

- basic security configurations must be established and applied for the design and development of applications, databases, systems, network infrastructures (developed or acquired) and

information processing must comply with applicable policies, standards and regulatory requirements.

- periodically, and at least once a year, the Supplier must initiate a review process of the security configurations applied in its infrastructure. Variants entered into the various configurations must be duly recorded.
- The Supplier must demonstrate that it has put in place an effective Patch Management process to address known vulnerabilities to the manufacturers of the assets that issue security patches for this purpose.
- The Supplier must prove that it has also activated, within the patch management process, the security procedures concerning the insertion of patches in its infrastructure. Such security operations must include test environments where application tests are to be carried out for the safe insertion of patches into one's own infrastructure.
- Patch management must include a prior risk assessment of the vulnerability being mitigated with the patch. The Supplier must demonstrate that it has a procedure for assessing and prioritizing the insertion of patches that takes into account the risk to be mitigated.

4.6. Physical security

The Supplier must have adequate physical security procedures in its premises and/or offices to cover the following areas:

- all visitors to the Supplier's Data Centres or to which the Supplier has access must be accompanied and wear a specific identification badge. The date and time of entry and exit must be recorded;
- The identity of visitors must be verified before entering a Data Centres;
- no visitor may be admitted to a Data Centres of the Company or to which the Company has access, without a confirmed appointment;
- the Supplier must establish appropriate procedures to ensure that responsibilities for maintaining a safe operating environment are properly assigned and fulfilled;
- the Supplier must apply physical and environmental controls to protect the service in a manner commensurate with the level of risk and indicate the physical and environmental threats identified during the risk assessment;
- the physical protection of service equipment and the service work area must include as a minimum:

    - systems for the detection and notification of illegal access;
    - Security of users from fire and other threats such as natural disasters (storms, tornadoes, etc.) and non-natural disasters (explosion threats, cyber-attacks and other accidental or malicious activities);

- sites where RGI Spa data or processes are managed must comply with generally accepted security standards (e.g. ANSI/TIA942) for Data Centres management and security.

5. Right of Audit

The Supplier must accept the restrictions and security measures of RGI Spa set out below:

- RGI Spa or its delegated personnel who have signed a non-disclosure agreement ("NDA"), may access the Supplier's sites subject to the Supplier's consent (in the event of a refusal, appropriate reasons must be provided) and to applicable security regulations; agreement on prior notice is to be given regarding the personnel, timing, duration and scope of the services provided and any refusal of access to persons delegated by RGI Spa in the event of a conflict of roles or impact on the Company's performance levels;
- RGI Spa reserves the right to conduct periodic audits of the physical security requirements of the environment;
- RGI Spa (or its delegated personnel) shall be entitled to inspect/audit regularly (at least once a year or at planned intervals) the security procedures and processes established within the services provided, which shall include as a minimum:
    - risk management process;
    - Incident and Change Management process;
    - security tests (VA and PT, SAST, DAST, etc);
    - Guidelines for the hardening of systems;
    - Secure Software Development Life Cycle (S-SDLC)
    - Business Continuity Plan and DR and other contingency processes and services.
- RGI Spa shall have the right to inspect, at no additional cost, the operational processes implemented by the service, based on environment, extension and third-party agreements;
- RGI Spa reserves the right to request changes to the Company's security processes if these are deemed inadequate. These changes must be mutually agreed upon, commercially reasonable and subject to acceptable deadlines;
- RGI Spa reserves the right to request auditors to produce audit reports to verify the risk management measures taken by the company providing the service, e.g. IT security and Penetration Test reports, vulnerability assessment, BCP/DR plan, software test reports, etc.
- RGI Spa reserves the right to request the annual completion of a self-assessment questionnaire for the purpose of assessing the Company's level of compliance with internal security measures.

Sede legale:
Via San Gregorio 34
20124 Milano
t +39 02 22190111
f +39 02 22190100

Capitale Sociale € 2.522.319 i.v.
P.IVA 13251500156
C.F. 06602910017

Sede amministrativa:
Via Cesare Pavese 6
10015 Ivrea, TO
t +39 0125 935111
f +39 0125 935100

info@rgigroup.com
www.rgigroup.com