



**IMS – Integrated Management System**

**ISO/IEC 27001:2013 - UNI EN ISO9001:2015**

**Policy on Information**

**Security, Personal Data**

**Protection and Quality**



# Gerico Security Srl

Prepared by: The Board of Gerico Security Srl

Date: 12/04/2022

Ver. 2.0

Information classification: Public

## TABLE OF CONTENTS

1	PURPOSE.....	3
2	Principles of the IMS.....	3
2.1	Management duties - Objectives .....	4
3	Realization of IMS.....	5
4	Policies on document protection .....	5
4.1	Review.....	5

Version	Date	Remarks
1.0	27/09/2019	First emission
1.1	19/11/2021	<b>Editorial review</b>
1.2	31/03/2022	Revision on Personal Data Aspects
2.0	12/04/2022	<b>Integration as IMS of Quality and Information Security Policy</b>



## 1 PURPOSE

Gerico Security Srl defines its policy on Information Security regarding an Information security and Quality management in compliance with ISO/IEC 27001:2013 and UNI EN ISO9001:2015:2015 and its Ethical Code. Gerico Security Srl implement its policies according to the principles of sustainable development, effectiveness, efficiency and quality of the internal processes and professional services provided to its clients.

## 2 PRINCIPLES OF THE IMS

Gerico Security has set out an Integrated Management System (IMS) for Information Security and Data Protection (ISMS) and Quality (QMS) in compliance with the law and applicable standards. The Integrated Management System is defined through a continuous risk analysis process aimed at ensuring adherence to its Ethical Code, its service quality and protecting its own information, clients' information and interested parties' information. The Company undertakes to continuously improve such processes and services also through its Integrated Management System for Information Security and Quality and according to its strategical objectives and Ethical Code, Quality. Business processes and the services provided to Clients are of primary importance to Gerico Security

Gerico Security ensures the protection of information according to its sensitivity, availability (where needed) and prevents unauthorised accesses or changes and protects data subject rights from impacts in adherence to the principle of Accountability ex art.5.2 GDPR.

In particular, Gerico Security Srl considers essential a consistent application of its Code of Ethics to guarantee the confidentiality and the protection of the clients' information and personal data therefore, it has structured its Information Security Management System (ISMS) to achieve the goals thereof.

Gerico Security ensures the resources needed, such as personnel, information, systems and infrastructures to protect confidentiality, integrity and availability of information throughout its activity. To this end, it carries out specific controls over information security in compliance with law on the legal protection of personal data in particular.

The Board ensures its commitment to the continuous improvement of its Information Security Management and Quality and adherence to the law and its Ethical Code.



## 2.1 MANAGEMENT DUTIES - OBJECTIVES

Gerico Security Srl has set out and maintains the IMS in compliance with ISO/IEC 27001:2013 and UNI EN ISO 9001:2015. Its objectives are as follows:

### A. Objectives of Information security:

- Protection of the Company and client information which is obtained, treated or produced throughout the professional services carried out, protecting information confidentiality, integrity and availability.
- Where necessary, ensure the appropriate access to the right information and avoid unauthorised accesses to Gerico Security Srl personnel and staff or of those who work in Partnership
- Set out and implement the ISMS security measures to protect information against breaches, misuse and frauds.
- Define internal and external roles and responsibilities for information security.
- Support personnel and staff by providing appropriate training and running courses in information security for security awareness and risk minimisation.
- Ensure information security continuity in case of an adverse scenario or if a threat takes place.
- Ensure compliance with the ISO/IEC 27001:2013 standard.
- Maintain adherence to contractual agreements, law and regulations on information security in particular.

### B. Objectives of Quality:

- adopt and implement principles and good practices to ensure the Quality of the company's processes and services to be provided in order to promote Certificates of compliance with standards;
- set out an Integrated Management System (IMS) in compliance with UNI EN ISO 9001:2015, aimed at providing Clients with the best possible service, based on quality processes;
- identify roles and responsibilities to be assigned to its staff regardless its hierarchical organization levels, also involving third party personnel with key roles;
- assign the resources needed to implement the appropriate measures for the Quality of internal processes and Client services;
- continuously promote the Integrated Management System through the constant commitment of those who have apical Positions and Functions;
- identify, formalize and apply the rules for the services to be provided in accordance with ethical and improvement principles;
- develop personnel awareness programs through periodic information and training sessions;
- prepare appropriate reaction and management measures in case of events which may have impacts on quality business process and on Quality Client services;
- adhere to the requirements of contracts, law and regulations as regards both the internal processes and the activities for the Clients;
- promote the development of and select professional providers in accordance with the Ethical Code and this Policy by making commitments to behave accordingly.





- make commitments to continuously improving the Integrated Management System by planning, carrying out, verifying and implementing measures and preventive actions from possible impacts on the processes and Client service Quality

### 3 IMPLEMENTATION OF THE IIMS

The IMS includes all policies and procedures implemented for the achievement of information security, Quality and Data Protection objectives.

The IMS scope encloses all activities and processes to provide operational, administrative and support activities.

All shareholders, employees, collaborators, providers, contractors, partners and third parties who treat Gerico's information or Gerico's client information are required to adhere to the present policy on information security, personal data protection and Quality. The Board of Gerico Security Srl is directly responsible for the policy implementation and adherence to the policy by the above parties.

The Board shares the principles and the objectives of the IMS and fully supports its implementation and maintenance by providing the resources needed to this end.

The Board approves and issues the present policy on security information, personal data protection and Quality which constitutes a programmatic document of reference for all the other IMS documents. Then, the Board communicates the policy and makes it available to all interested parties as needed.

### 4 POLICIES ON DOCUMENT PROTECTION

Gerico Security Srl has drew up, approved, published and communicated the present policy and suitable internal documentation regarding information Security, personal data protection and Quality to employees and interested parties.

The policies are made available on the Company's official website. The documents of the IMS can be shared with third parties and made available upon request.

In addition, Gerico Security Srl periodically provides the documents needed to monitor and track the IMS status of performance and adherence to standards, law, regulations and contractual terms in force.

#### 4.1 REVIEW



This policy is periodically reviewed and/or in the case of significant changes which might have impacts on information security and personal data protection for the purpose of ensuring appropriateness, adequacy and effectiveness and adherence to law and standards.

**GeRiCO Security Srl**

27/09/2019

**The Management Board**