



IMS – Integrated Management System
ISO/IEC 27001:2013 - UNI EN ISO9001:2015

Policy on Information
Security, Personal Data
Protection and Quality

Prepared by: BoD Gerico Security Srl
 BoD Gerico Lab Srl

Date: 08/07/2023

Ver. 4.0

Classification: Public Use

| Version | Date | Remarks |
|---------|------------|---|
| 1.0 | 27/09/2019 | First emission |
| 1.1 | 19/11/2021 | Editorial review |
| 1.2 | 31/03/2022 | Revision on Personal Data Aspects |
| 2.0 | 12/04/2022 | Integration as IMS of Quality and Information Security Policy |
| 3.0 | 07/06/2023 | IMS extension to Gerico Lab Srl |
| 4.0 | 08/07/2023 | IMS policies review |

Table of contents

| | |
|---|----------|
| 1 PURPOSE..... | 3 |
| 2 PRINCIPLES OF THE IMS..... | 3 |
| 2.1 MANAGEMENT DUTIES - OBJECTIVES..... | 4 |
| 3 IMPLEMENTATION OF THE IMS..... | 5 |
| 4 POLICIES ON DOCUMENT PROTECTION..... | 6 |
| 4.1 REVIEW | 6 |

1 PURPOSE

Gerico Security Srl and Gerico Lab Srl adopt their security information and quality policies in accordance with ISO/IEC 27001:2013 and UNI EN ISO9001:2015 in compliance with their Code of Ethics. Gerico Security Srl and Gerico Lab Srl implement the above policies according to principles of sustainable development, effectiveness, efficiency and quality of internal processes and activities provided to their clients.

2 PRINCIPLES OF THE IMS

Gerico Security has established an Integrated Management System that includes all the Company's policies as regards the relevant aspects of delivery and management of internal activities and services that the Company provides to its clients. In particular, the integrated policies are listed as follows:

- Information Security
- Quality
- Occupational health & safety in conformity with the law and in terms of corporate welfare
- Gender Equality
- Environmental Sustainability and Energy Efficiency

The Integrated Management System includes the above Policies ensuring compliance with the Group's Code of Ethics provisions, the set of principles and rules pertaining the business and the Group's activities. (Code of Ethics is made available to interested parties: disseminated throughout the group and published on the company website).

The Integrated Management System is extended and adopted by both the parent company Gerico Security Srl and its subsidiaries to ensure adherence to the Group's Code of Ethics provisions, the quality of the services, the protection against threats to information assets of the Group, of clients and interested parties interacting with the Group in various ways.

Considering the activities conducted for the clients, the Group's clients consider some aspects of the Policies as vital and ensured through third-party assessment and monitoring in conformity with international certifications. In particular, the processes of Information Security Management System (ISMS) and Quality (QMS) are ISO/IEC27001 and ISO 9001certified.

This Policy regards the two aforesaid Information Security and Quality Management systems.

Gerico Security Srl and Gerico Lab Srl undertake to continuously improve the above processes and services through the Integrated Management System for Information Security and Quality according to strategical objectives, the Ethical Code and Quality. The

business processes and services provided to Clients are of primary importance to Gerico Security and Gerico Lab.

Through a continuous risk assessment process, Gerico Security ensures the protection of the Group information according to information sensitivity, availability (where needed), prevents unauthorised accesses or changes and protects the 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 and Gerico Lab ensure the resources needed, such as personnel, information, systems, and infrastructures to protect and uphold confidentiality, integrity, and availability of information while conducting business and professional activities. They carry out specific information security controls in compliance with law on the protection of personal data accordingly.

The BoD of each Company ensures commitment to the continuous improvement of its Information Security Management and Quality, adherence to the law and to its Ethical Code.

2.1 MANAGEMENT DUTIES - OBJECTIVES

Gerico Security and Gerico Lab have set out and maintain the IMS in compliance with ISO/IEC 27001:2013 and UNI EN ISO 9001:2015. The objectives are as follows:

A. Objectives of Information security:

- Protection of the Company and client information, obtained, treated, or produced throughout the professional services provided, information security, confidentiality, integrity, and availability.
- Where necessary, ensure the appropriate access to the right information. Avoid personnel, staff or those who work in Partnership unauthorised accesses to information.
- 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.

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 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 IMS

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 information of Gerico Security Srl, Gerico Lab Srl, and their clients' information, are required to adhere to the present policy on information security, personal data protection and Quality. The BoD of Gerico Security and Gerico Lab Srl is directly responsible for the policy implementation and adherence to the policy by the above parties.

The Board of the Companies 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 of Gerico Security and Gerico Lab Srl 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, it communicates the policy and makes it available to all interested parties as needed.

4 POLICIES ON DOCUMENT PROTECTION

Gerico Security Srl and Gerico Lab Srl have drawn 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 and Gerico Lab Srl periodically provide 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.

Monza, 08/07/2023

GeRiCO Security Srl

Gerico Lab Srl

Board of Directors

Board of Directors