

HORIZON CONSULTING			
Issued by: C&ISO	Document ID POL006	Version 4.0	Date 02/01/2025



POL006

QHSE & Information Security Policy

			
Issued by: C&ISO	Document ID POL006	Version 4.0	Date 02/01/2025

Content index

- 1 Overview 3**
 - 1.1 Background 3
 - 1.2 Objectives..... 4
 - 1.3 Scope 4
 - 1.4 Validity and maintenance 4
 - 1.5 References..... 5
 - 1.5.1 Standards and regulations 5
 - 1.5.2 Internal regulations 5
- 2 Quality & Information Security Policy 6**
- 3 Roles and responsibilities 8**
- 4 Revision history 9**
- 5 Glossary 10**

			
Issued by: C&ISO	Document ID POL006	Version 4.0	Date 02/01/2025

1 Overview

1.1 Background

Horizon Consulting S.r.l. and its subsidiaries Horizon Security S.r.l. and Horizon Digital S.r.l. (hereinafter “Horizon Group” or the “Group”) are engaged in Cybersecurity and Digital Transformation consulting.

Operating primarily in an Enterprise market that is highly demanding in terms of:

- expected quality of services provided;
- cutting edge for risk scenarios on information assets;
- dynamism of services offered;
- skills, knowledge and capabilities of the highest level;
- timeliness and effective resolution;
- differentiation and uniqueness from local or global competitors;

interacting with Regulatory Bodies and Professional Associations aimed at:

- standardize best practices;
- address cybersecurity and digital transformation approaches, methodologies and solutions;
- updating and evolving regulations, laws, and standards with respect to the applied regulatory and best practice environment;

collaborating with Vendors and Partners to:

- structure integrated cybersecurity and digital transformation services;
- bring new solutions and technologies to market;
- automate processes, procedures and security measures;
- ensure data protection;
- build mutually beneficial relationships;

having relationships with Supervisory Authorities and Public Authorities:

- in inspections, audits activities
- for reporting activities

The Horizon Group through the Group Board is committed to:

- constantly elevate the Quality of Service while simultaneously
- respect the environment and help ensure its protection
- ensure the health and safety of its employees and all partners who work with the company
- protect the Information Security of all stakeholders, primarily the customers.

Customer satisfaction, both in terms of the quality-of-service delivery and security in processing the business data that concerns them, must be the driving force behind the activities of the Horizon Group the interpretation of needs and its satisfaction, are, in fact, placed at the center of every decision.

			
Issued by: C&ISO	Document ID POL006	Version 4.0	Date 02/01/2025

The Horizon Group also emphasizes that the very essence of the Group is its employees, who are the first customer. Staff must be motivated and involved in activities. A team of close-knit, organized, technically prepared and customer-oriented people must be built and maintained, capable of mastering all problems and aspects of daily business life at all times.

It is necessary for internal processes to be sustainable and human-scale, and for this to be constantly oriented toward improvement, both in technological and training aspects, with a view to management aimed at, increased productivity, improved service and safety perceived by the customer.

Internal staff satisfaction is undoubtedly an indispensable element of accelerating the company's strategic objectives, a starting point for measuring the company's success in the market.

Hence the need to enhance specific aptitudes through the involvement and training of staff on multiple issues, most notably the Quality of Service Delivered and Information Security.

1.2 Objectives

The purpose of this Policy is to define principles, objectives and values that must be adopted in order to direct the achievement of business objectives and to guarantee an adequate level of protection of the company business, specifically:

- affirming business values;
- defining the high-level goals for the business;
- emphasizing the need for employees to be competent;
- addressing risk management;
- having customer satisfaction firmly in mind;
- providing guidance toward continuous improvement;
- comply with the rules and laws applicable to the company;
- protecting customers' data.

1.3 Scope

This Policy applies to the following subjects:

- to all internal company personnel (employees with fixed-term/permanent/apprenticeship contracts, interns, temporary workers, etc.);
- to third parties (eg: external collaborators, partner companies) who collaborate in various capacities with *Horizon Consulting* in carrying out business activities.

1.4 Validity and maintenance

This document takes effect from the date of its issue and is communicated to the company personnel involved by e-mail and published on the company intranet.

The document is valid for one year, expiring on 31 December of each year.

			
Issued by: C&ISO	Document ID POL006	Version 4.0	Date 02/01/2025

During this period, the Company Management has the right to integrate/modify the content of this procedure, communicating any changes to the company personnel by e-mail and publishing the updated version of the document on the company intranet.

1.5 References

1.5.1 Standards and regulations

This Policy takes into due consideration the requirements expressed by the following laws and regulations:

- Regulation (EU) 2016/679 (GDPR) concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data;
- Legislative Decree 196/2003 (as amended by Legislative Decree 101/2018) - Code regarding the protection of personal data (Privacy Code) and Provisions issued by the Guarantor for the protection of personal data;
- Legislative Decree 231/2001 on the regulation of the administrative liability of legal persons, companies and associations also without legal personality

This Policy refers to the indications contained in the following international standards:

- ISO 9001:2015 Quality management systems – Requirements
- ISO 14001:2015 Environmental management systems – Requirements
- ISO/IEC 27001:2017 Information Technology - Information security management systems – Requirements;
- ISO/IEC 27002:2013 Information Technology - Code of practice for information security management.

1.5.2 Internal regulations

This Policy refers to the following company regulations and documents:

- *Horizon Consulting - IMS001 - Management System Manual*
- *Horizon Consulting - IMS002 - QHSE Manual*

			
Issued by: C&ISO	Document ID POL006	Version 4.0	Date 02/01/2025

2 QHSE & Information Security Policy

The Horizon Consulting Group Board identifies the implementation of the integrated Information Security and QHSE Management System, according to ISO 9001, ISO 14001 and ISO/IEC 27001, as a very important stimulus to achieve the objectives of its business strategy.

Obtaining and maintaining certifications of its integrated Information Security, Quality and Environmental management system remain key objectives of the company's growth.

The Horizon Consulting Group pursues the continuous improvement of its Quality, Environmental and Information Security Management System by identifying the following principles:

1. recognizes that commitments made to its customers and all other stakeholders, **exceeding their expectations** constitute ongoing obligations for the entire company.
2. assumes as a priority the **quality of the relationship** with the customer, also recognizing the importance of relationships with suppliers and partners and their enhancement, with a view to common growth.
3. is committed to **constant motivation and training** of human resources.
4. **recognizes the professional and human value of its employees** as the company's assets and is committed to constant enhancement and promoting transparency of relationships.
5. recognizes that the **quality is decisive** for the realization of the company's business, and for the creation of value for its customers.
6. recognizes that the **environment is a common good** to be protected through compliance with laws and targeted actions that bring positive benefits to the planet and stakeholders.
7. undertakes to plan, develop, update and **communicate the objectives** of the Quality and Information Security Management System in order to improve its implementation and compliance with applicable laws and regulations.
8. provides a fundamental **support service** to the company's Core Business through tools and means that are technologically in line with progress and maintain them in efficiency;

			
Issued by: C&ISO	Document ID POL006	Version 4.0	Date 02/01/2025

9. **establishes roles and responsibilities** of personnel involved in Quality and Information Security management;
10. periodically and systematically **identifies threats, vulnerabilities** looming over business objectives and information, assessing their risk exposures and implementing appropriate treatment actions;
11. **trains personnel** in the performance of activities so as to protect corporate assets in compliance with current regulations;
12. encourages the dissemination of the **culture and awareness of data and information security and protection**, especially the confidentiality, integrity and availability of data and information, among its employees, collaborators, partners and third parties regarding their roles and responsibilities in this area;
13. **cope promptly, effectively and scrupulously with emergencies or incidents** that might occur in the performance of its activities, also cooperating with third parties or appointed entities;
14. **complies with the laws and regulations** in force in this context, and in any case adheres to standards identified with a sense of responsibility and awareness, based on scientific principles and from risk assessment;
15. conducts **monitoring and review activities**, starting with the most critical ones, to update programs for achieving and ensuring this policy;
16. undertakes **continuous review of the Integrated QHSE and Information Security Policy** to maintain its suitability and disseminate it along with its objectives;
17. ensures that **all personnel at all levels understand its contents** and are committed to abiding by it.

			
Issued by: C&ISO	Document ID POL006	Version 4.0	Date 02/01/2025

3 Roles and responsibilities

Below are the main roles and related responsibilities that play a key role in ensuring the correct implementation of the *Policy*.

Group Board

The *Group Board* defines the strategies, objectives and guidelines for the management system and:

- approves and supervises the application of the "*Quality and Information Security policy*";
- ensures the consistency of this *Policy* with the other corporate regulations.

C&ISO / QHSE Manager

The *C&ISO and QHSE Manager* are responsible for the following tasks:

- defines and updates the "*Quality, Environmental & Information Security Policy*";
- ensures consistency and compliance between the security measures indicated in the *Policy* and their application on the systems;
- supports the *Company Departments* in identifying and adopting measures necessary to meet the requirements expressed by this *Policy*.

HORIZON CONSULTING			
Issued by: C&ISO	Document ID POL006	Version 4.0	Date 02/01/2025

4 Revision history

Version	Date	Action	Author	Verified By	Approved by
1.0	26/03/2016	Drafting and issuing of the first version of the document	IT	CEO	CEO
2.0	31/05/2023	Review and update of the Policy	C&ISO	CEO	CEO
3.0	01/12/2023	Quality and Information Security Policy integration	C&ISO / Quality Manager	Group Board	Group Board
3.1	06/03/2024	Changes for external publication. <i>(Impl. Rec #2 ISO/IEC 27001 Phase 1 Certification Audit)</i>	C&ISO / Quality Manager	Group Board	Group Board
4.0	02/01/2025	Introduction references to ISO 14001	QHSE	Group Board	Group Board

HORIZON CONSULTING			
Issued by: C&ISO	Document ID POL006	Version 4.0	Date 02/01/2025

5 Glossary

The main technical terms used in this Policy are listed below.

Term	Description
Availability	Ownership of making information accessible and usable according to the times and methods required by an authorized entity.
Integrity	Characteristic understood as the ability to safeguard the authenticity and completeness of the information.
Confidentiality	Property that ensures that information is not made available or disclosed to unauthorized individuals, entities or processes.