GRUPPO ZENIT

General policies for Quality and Information Security

Gruppo Zenit S.r.l. is a Managed Service Provider: it provides IT services in managed mode on Private Cloud infrastructures in IaaS, PaaS, SaaS modes; guarantees 24/7 monitoring, 24/7 SPOC, Incident and Problem Management. Furthermore, it offers its thirty years of experience in the field of IT consultancy for Digital Transformation and Change Management.

The Top Management of Gruppo Zenit has drawn up a Quality and Security Policy through which to provide the services described above, guaranteeing the quality and security of information. The strategic direction, principles, basic rules and objectives of this Policy have been defined in order to achieve three primary objectives:

1. Achieve customer satisfaction;
2. Ensure the protection of its information assets and human resources, minimizing the risk of damage caused by deliberate or involuntary security incidents from within, from outside or from potential threats;
3. Pursue continuous improvement objectives.

Furthermore, through the application of this policy, Gruppo Zenit intends to comply with the principles and controls established by ISO 27001, ISO 27017 and ISO 27018, or other standards/regulations that govern the business activities in which the company operates, among such as, in particular, the regulations relating to privacy and security of personal data (GDPR).

Responsibility for the application of this Policy concerns the entire company organization, from the Top Management down to each individual employee. This application takes place in compliance with current laws and provisions, contractual requirements, company rules and procedures.

Customer satisfaction

Customer satisfaction is the basis of the strategies identified as it is fundamental to the consolidation of the company's reputation and its brand identity. Customer satisfaction is guaranteed through:

1. Provision of services and supply of quality products that satisfy the initial and subsequent needs and expectations of customers, in relation to the agreed price and in a highly competitive position compared to the best and fairest competition.
2. These services and products are provided in compliance with punctuality, cost control, continuity of provision, compliance with laws and regulations, application of best practices and standards, continuous updating and customer documentation. Demonstrating to stakeholders its ability to regularly provide safe products/services, maximizing business objectives.
3. In support of a quality service, Gruppo Zenit interprets and approaches projects in the form of standardized processes. This approach guarantees performance

optimization, greater control over the progress of the project and the resources necessary to achieve the objectives, allows you to establish objectives, roles and responsibilities upstream as well as calculate and predict possible risks and the related mitigation solutions.

Protection of information assets

The protection of the information assets of Gruppo Zenit and its customers is placed at the center of the conservative and protection strategies, placing confidentiality, integrity and availability at the center of these strategies, preparing investments aimed at guaranteeing security and protection of the information system, reducing the risk of accidents, minimizing the risk of loss and/or unavailability of customer data, planning and managing activities to guarantee service continuity. These safety and protection objectives are pursued through:

1. Identification of risks, through a continuous and adequate risk analysis that constantly examines the vulnerabilities and threats associated with the activities to which the system is applied, in order to understand the vulnerabilities and possible threats present in the company that can expose it to risks failure to achieve objectives.
2. Risk management to an acceptable level through the design, implementation, and maintenance of appropriate countermeasures for information security, to ensure the quality of the products and services provided and for the health and safety of the workplace.
3. Adoption of security requirements, in particular for the implementation and provision of cloud services, pursuant to ISO 27017. Gruppo Zenit undertakes to adopt these requirements by taking into consideration the risks deriving from internal staff, the secure management of multi-tenancy (infrastructure sharing), access to cloud assets by service provider personnel, access control (in particular administrators), communications to stakeholders in the event of changes to the infrastructure, security of virtualization, data protection and access in the cloud environment, cloud account life cycle management, communication of data breaches and guidelines for sharing information to support investigation and forensic activities, as well as constant security on the physical location of the data on cloud servers.
4. Protect the confidentiality of information by ensuring that the information is:
    1. accessible only to those authorized to do so;
    2. precise and complete;
    3. available to those who have access rights.
5. Timely and effective actions in response to emerging needs during work activities.
6. Identification of dangers and risks present within the organization.

Furthermore, Gruppo Zenit, in its strategies for safeguarding information assets, pays the utmost attention to the protection of personal data. The data entrusted to Gruppo Zenit by customers, suppliers, employees and collaborators are managed in compliance with the laws and regulations applicable to data protection and always with a view to continuous updating according to best practices regarding new technologies. The Gruppo Zenit's commitment to the protection of personal data is based on principles of: transparency and clarity; legal basis; data minimization; data security; rights of the interested party; training and awareness; limited data retention; vulnerability and penetration testing; external audits; guarantees to customers and suppliers. In particular, with its customers, the company,

pursuant to ISO 27018 and current privacy legislation (GDPR), acts as "Data Processor", declaring this status and the related obligations that derive from it in contracts with customers. These obligations are also reported in the data processor agreement.

The Top Management and the managers of each department are committed to ensuring that the principles outlined above are effectively applied at every step of the production process and in the services that Gruppo Zenit offers to its Customers, as well as towards its Suppliers and its staff.

Continuous improvement

The continuous improvement of Gruppo Zenit's system is based on involvement, cooperation and collaboration between company resources. This primary objective is pursued through:

1. Periodic review of the Policy, Objectives and implementation of the System.
2. A process vision that takes into consideration the organizational context and management strategies, the planning of objectives, the management of resources, assets, policies and procedures, the criteria for self-assessment and internal verification of the organization and the stimuli towards such improvement.
3. Attention to the surrounding environment, relying on a preventative approach to problems rather than on subsequent control and related correction, in order to significantly reduce the probability of accidents, injuries or other non-compliances occurring.
4. Training and updating of staff, maintaining high levels of performance, ability to respond to changes and identify new growth opportunities.
5. Involvement of staff, welcoming their contributions and reports, in a working environment open to constructive communication and open to dialogue.
6. Promotion of collaboration, understanding and awareness of the System by strategic suppliers.

This policy is formulated and reviewed by the Top Management of the company. All staff, based on their knowledge, have the responsibility to report any weak point identified in the company systems to the System Manager. This policy is reviewed regularly to identify any changes that affect it and to ensure that it remains suitable for the organization's purposes and the expectations of stakeholders.

Novara, 30/10/2023

The Top Management