# Information Security Policy

CENTRIC

# Information Security Policy

### Scope

The purpose of this document is to describe the general information security principles defined by IT CENTRIC, in order to develop an efficient and secure Information Security Management System (ISMS), establish the reference framework for the objectives to be pursued and Management's commitment to meeting applicable requirements and continuously improving performance.

### Application Scope

The information security policy applies to all internal and third-party personnel who collaborate in the management of information and to all processes and resources involved in the planning and provision of in-person and remote training services. The reference office is Corso Trieste, 291 81100 Caserta (CE).

### Generality

For IT CENTRIC, information security management has the primary objective of preserving the confidentiality, integrity and availability of information, in order to safeguard the assets represented by company assets and knowledge, satisfy the requirements of interested parties and protect people physical entities whose personal data are processed. Due to the characteristics of the services that the company offers to its customers and the value that information represents in its business, the information security policy represents a fundamental and priority strategic direction. To pursue the primary objective, the Management pays great attention to the design, management and maintenance of its technological, physical, logical and organizational structure. The Management therefore commits its organization to developing and maintaining a management system for information security within the scope of the activities carried out and the services provided in accordance with the requirements of the ISO/IEC 27001 standard, which represents the international reference standard to preserve the confidentiality, integrity and availability of the information.

### General principles of information security

All people who work and/or collaborate with IT CENTRIC are committed to respecting the following principles:

1. **Confidentiality:** ensuring that the information is accessible only to duly authorized individuals and/or processes and that the information is not made available or disclosed to unauthorized persons or entities.
2. **Integrity:** safeguarding the consistency of the information from unauthorized modifications and guaranteeing that the information does not undergo modifications or

deletions following errors or voluntary actions, but also following malfunctions or damage to technological systems.

3. **Availability:** ensure that authorized users have access to information and associated architectural elements when they request it.
4. **Control:** ensure that data management always occurs through safe and tested processes and tools.
5. **Authenticity:** guaranteeing a reliable provenance of the information.
6. **Privacy:** ensuring the protection and control of personal data.

The Management is strongly committed to making all the people who work for and with IT CENTRIC highly responsible in guaranteeing the rigor of their work to fulfill the assigned tasks with the utmost attention. The final responsibility for information security falls on the Management which has delegated the Manager of the integrated management system, the IT Manager and the representatives of each organizational unit involved to implement what is necessary.

**General framework for information security objectives**

The Management defines the following reference framework to determine the objectives for information security:

information critical for the company's business and personal data considered particular (art. 9 of EU Regulation 2016/679) must be protected by suitable security measures to be periodically re-evaluated based on the risk assessment.

the personal data, which IT CENTRIC holds in any capacity (Data Controller or Data Processor appointed by external Data Controllers) must be processed in full compliance with legal obligations (EU Regulation 2016/679 on the protection of personal data; national regulations and provisions regarding the protection of personal data).

the data and information must be protected, through the implementation of suitable logical, physical and organizational countermeasures, from unauthorized access.

the data and information must retain the characteristics of inalterability during processing operations.

the data and information contained in the information systems must be readily available to authorized users when they request them.

it is necessary to ensure compliance with all the parameters for measuring the quality of the services provided as defined in the contracts (SLAs) and in the SGSI documentation.

safety objectives must be measurable and established based on:

the results of the risk assessment, periodically and systematically updated on the basis of data from the monitoring and functioning of the SGSI.

the legal requirements imposed by national and community legislators; the contractual requirements that IT CENTRIC has accepted towards its clients.

company staff must receive training on data processing methods and information security; IT CENTRIC must operate in full compliance with the law on intellectual property rights when using commercial software packages and other material covered by copyright.

IT CENTRIC must update its antivirus programs to prevent computer virus attacks, with a frequency strictly related to the releases of the qualified supplier.

IT CENTRIC adopts a set of countermeasures to prevent malicious software.

IT CENTRIC adopts a security incident management and reporting policy to those responsible, to guarantee the continuous operation of processes critical to its business.

**Management commitments.**

The security policy concretely represents the Management's commitment towards customers and third parties to guarantee the security of information, physical, logical and organizational tools suitable for processing information in all activities.

With this policy, the Management undertakes to ensure that:

1. the organization has full knowledge of the information managed and evaluates its criticality from time to time, in order to facilitate the implementation of adequate levels of protection.
2. access to information occurs in a safe and suitable manner to prevent unauthorized processing or processing carried out without the necessary rights.
3. the organization and third parties collaborate in the processing of information by adopting procedures aimed at respecting adequate levels of security.
4. the organization and third parties who collaborate in the processing of information are adequately trained and have full awareness of security issues.
5. anomalies and incidents having repercussions on the information system, services and corporate security levels are promptly recognized and correctly managed through efficient prevention, communication and reaction systems in order to minimize the impact on the business.
6. access to the headquarters and individual company premises is carried out exclusively by authorized personnel, to guarantee the safety of the areas and assets present.
7. compliance with legal requirements and compliance with the safety commitments established in contracts with third parties are ensured.
8. the detection of anomalous events, incidents and vulnerabilities of information systems are managed in order to respect the security and availability of services and information.
9. corporate business continuity and disaster recovery are implemented through the application of established security procedures.
10. the processing of personal data, both in cases in which the company operates as Data Controller and in cases in which it operates on behalf of third parties as Data Controller, takes place in compliance with the European Regulation on the Protection of Personal Data GDPR 679/2016.

**Finally, the IT CENTRIC Management undertakes to:**

- adopt a secure information management system compliant with the specified requirements of ISO/IEC 27001.

- constantly monitor the degree of compliance of the system with the applicable rules and laws of a mandatory and voluntary nature, and the contractual obligations pertaining to the scope of application of the SGSI.
- guarantee suitable means and resources for its maintenance and continuous improvement, in particular with regard to the mitigation/reduction of risk levels on information security and the adoption of suitable measures to prevent anomalous and emergency situations.
- make all people in the organization aware of the obligations and responsibilities of each in the management of information security and of the consequences in the event of events, whether malicious or negligent, relating to the unauthorized use, modification or destruction of critical information.

The information security policy is constantly updated and verified, through an annual review, to ensure consistency with the strategic aims of the organization. The policy is shared with the organization, third parties and customers, through its publication on the site.