**DATA SECURITY POLICY**

**ALTER EGO** recognizes the need to ensure the information goods that are in her possession or under her control as well as the obligation to comply with the Greek and European legal and regulatory framework.
The Security Policy is the framework for data protection managed by ALTER EGO, providing guidance to the Organization on how to organize and process information. The Security Policy consists of a set of rules that define the way in which ALTER EGO manages and protects her Information Assets. These rules define the role of each stakeholder within the company, its responsibilities, blames and duties.
As every society needs laws and guidelines / instructions for its safety and proper operation, every company/organization needs a specific Security Policy (PA) that ensures the reliable, organized and effective use of information resources.
The purpose of the Security Policy is the SAFE, RELIABLE AND INDEPENDENT provision of services and products to final customers or cooperating entities.
The aim of the Security Policy is to establish a framework of general guidelines for the protection of ALTER EGO information, the implementation of which ensures an acceptable level of Security for the Organization in relation to its risk profile.
In addition, the aim of the P.A. is to place restrictions on the access and use of computers, information systems, networks, electronic means of communication and other relevant information media used for the storage and processing of data, documents and software that ALTER EGO owns and uses with the ultimate aim of ensuring the availability, integrity and confidentiality of information and information goods.

The primary objectives of the Security Policy are also:

- Ensuring the confidentiality, availability and integrity of information managed by ALTER EGO
- Ensuring the rights of individuals receiving services from European Reliance as well as its employees and associates
- Early identification of Information Security risks and their effective management
- Immediate response to Information Security incidents
- Ensuring the smooth operation of information resources
- Continuous improvement of the level of Information Security
- Meeting regulatory and legislative requirements
- the level of awareness of staff on risks that threaten Information Security and the continuous updating of best practices to be followed to minimise the likelihood of their occurrence.

For this reason ALTER EGO takes the necessary measures at technical and organisational level to ensure the integrity, availability and confidentiality of the information it processes. At the same time, it implements policies and procedures in which:

- Define the organisational structures necessary to monitor Information Security issues
- Technical measures to control and restrict access to information and information systems are defined
- Determine how information is classified according to its importance and value
- Describe the necessary actions to protect information during the processing, storage and distribution of information
- The ways of informing and training the Company's employees and partners in Information Security matters are defined
- Identify how to deal with Information Security incidents
- Describe the ways in which the safe continuity of the Company's operational functions is ensured in the event of computer system malfunctions or disasters

ALTER EGO shall carry out assessments of the risks associated with Information Security at regular intervals and shall take the necessary measures to address them. It implements a framework for assessing the effectiveness of Information Security procedures through which performance indicators are defined, their measurement methodology is described and periodic reports are produced which are reviewed by the Agency's Management with a view to continuously improving the system.
The System Manager in cooperation with the Information Security Officer of the parent company is responsible for the control and monitoring of information security policies and procedures and for taking the necessary initiatives to eliminate all those factors that may compromise the availability, integrity and confidentiality of ALTER EGO information.
All employees of ALTER EGO and its partners with access to information and information systems of the Company, are responsible for compliance with the rules of the applicable Information Security Policy.

THE CHIEF EXECUTIVE OFFICER
Konstantinidis George