1. Scope of Implementation of the Information Security Management System (ICSD)

The Information Security Management System (ISMS) applies to the following scope (hereinafter referred to as "Services").

«**SUPPLYING OF SERVICES IN RECORDING & REQUIREMENT ANALYSIS OF TELECOMMUNICATIONS & INFORMATION TECHNOLOGY INFUSTRUCTURES AIMING AT THE SUPPORT OF BUSINESS NEEDS & THE ACHIEVEMENT OF OPERATIONAL OBJECTIVES – TRADING, IMPORT EXPORT, REPRESENTATION & DISTRIBUTION OF HIGH TECHNOLOGY PRODUCTS AND SYSTEMS FOR MEASUREMENTS OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS- SUPPLYING OF SUPPORT, MAINTENANCE & EDUCATION SERVICES, RELATED TO THE TRADING OBJECTS AND PRODUCTS – HIRING & RENTAL OF MACHINES, TOOLS & SERVICES OF INFORMATION TECHNOLOGY & COMMUNICATIONS.**

2. Abbreviations

GISP: General Information Security Policy (in this document)

ISO: Information Security Officer

3. Scope of Policy

GISP applies to all Company personnel involved in the execution of the *Services* as well as in the use of equipment that is used by the Company for the execution of the *Services*, including any additional terms of the relevant contracts.

4. Legal and Regulatory Framework

The Legal and Regulatory Framework is determined by:

Law 4624/2019 (Protection of the individual from the processing of personal data, incorporating the amendments).

Regulation (EU) 2016/679 of the European Parliament and of the Council as per 27 April 2016 on the protection of individuals regarding the processing of personal data and the free movement of such data and abolition of Directive 95/46 / EC (General Data Protection Regulation)

Law No.2121 Gazette 25 A / 04-03-1993 Law for the Protection and Avoidance of Theft of Intellectual Property

Law 3741/2006 Law for the protection of personal data and privacy in the electronics sector.

ISO / IEC 27001: 2013 (Information Security - Information Security Systems - Requirements)

Note: The Company is committed to not accepting any contractual term that violates the above Legal and Regulatory Framework.

5. Scope

The Company seeks to provide the *Services* in accordance with the applicable Legal and Regulatory Framework and other contractual obligations in a way that protects the *information* from intentional or unintentional theft, destruction, or use in violation of the Laws and Regulatory Provisions.

The purpose of information security is to ensure the Company's business continuity and minimize the risks that threaten information, avoiding security incidents and reducing the impact that these incidents may have.

6. Policy

The purpose of this policy is to protect the information assets [1] of the Company and its customers from all internal, external, voluntary or unintentional threats.

The Company's specific objectives regarding Information Security are the below:

- ✓ The Information to be protected against any unauthorized access
- ✓ To ensure the confidentiality of Information
- ✓ To maintain Integrity of Information
- ✓ To Maintain the availability of Information
- ✓ To ensure compliance with statutory requirements
- ✓ To develop, maintain and test Business Continuity Plans
- ✓ To provide training on Information Security for all staff
- ✓ All real or suspected security incidents should be reported to the ISO and be fully investigated

In order to achieve the above objectives, specific Security Policies and Procedures have been developed and applied, describing all relevant personnel responsibilities. All staff and external partners (if required) are required to apply all Security Policies that fall into the scope of their activities.

Management is committed to providing all necessary resources and means to apply the present as well as the specific Security Policies.

7. Responsibilities

a) Management Responsibilities

The main responsibilities of the Management in relation to the management of the Information Security in the Company are:

- The formulation of the Company's policy in relation to Information Security.
- The approval and review of Information Security Policies, as well as the relevant Procedures and Guidelines.

[1] Information assets may exist in various forms, including data stored on computers, transmitted over networks, printed or written on paper, faxed, stored in disks or other storage media

- Approval of Risk Management Plans and Emergency Management Plans
- Ensuring the resources required for the effective implementation of the Information Security Management System.
- Creating the necessary conditions in the company to promote understanding of the role and responsibilities associated with Information Security. by staff
- The concern for the continuous improvement of the Information Security Management System
- Decision making regarding imposing sanctions in cases of disciplinary offenses in relation to Information Security.

7.2 Responsibilities of the Information Security Officer

Information Security Officer, is the representative of Management responsible for the Information Security Management, is the designated by Management, and in addition to his other duties, he has the following responsibilities:

• Collaborating with the Management for the development of Security Policies, Procedures and Standard Methods, in accordance with the Company's General Security Policy.

• Ensuring the implementation, maintenance and monitoring of Security Policies as well as compliance with regulatory requirements, applicable law and standards requirements

- Informing the Management on the performance and improvement of the Security Policies
- Updating company's information list and rating (List of information assets), in cooperation with the relevant business executives.
- Coordinating Information Security Management Team to identify and evaluate the threats related to the Company's information assets in cooperation with the relevant business executives
- Working with the Management and the Information Security Management Team to determine the necessary controls to address the risks.
- Monitoring and reporting to the Management of any security incident and activation of the relevant plan and strategy to address and avoid recurrence.
- Monitoring of the effectiveness of controls applied to address risks and report to Management.
- Organizing and conducting Internal Audits to control the effectiveness of the System.
- Contacting with external Bodies in relation to Security Management according to the relevant Policy.
- Ensuring personnel training on Security Management takes place and stresses the importance of participating in the implementation of the System.
- Preparation and coordination of the Review of the ISMS (Information Security Management System) by Management.

ISO reports directly to Management on all matters related to Information Security and is authorized to act on its behalf on them.

7.3 Information Security Management Group Competencies

Members of the Information Security Management team are defined the following:

- The Chief Executive Officer
- MSSQEH (Management System Supervisor for Quality, Environment & Health)
- The Information Security Officer (ISO)
- IT Manager

The main responsibilities of the Information Security Management Team are:

- Examining the Company's activities that fall within the scope of the ISMS (Information Security Management System) and identifying the information assets involved and the threats that threaten them.
- Assessing and evaluating the dangers of the identified risks.
- Reviewing proposals and listing control measures to address risks.
- Periodic review of the effectiveness of risk management plans.
- Detection of emergency situations and coordination of actions for the drawing up and approval of contingency plans.
- Reviewing the effectiveness of emergency plans

7.4 Responsibilities of Directors of Organizational Departments.

The main responsibilities of the Company's Directors of Departments in relation to the management of Information Security in the company are the below:

- Participation in identifying, assessing and planning the management of the risks associated with the IT assets managed by their Unit.
- Supervision of compliance with Security Policies by the staff of their Department.
- Active participation in the review of relevant safety incidents in order to investigate their causes and design the necessary corrective actions.
- Identify significant changes and trends that may affect Information Security practices in their area of responsibility and co-operate with the ISO and Management to adapt to new conditions.

7.5 Staff Responsibilities

The main responsibilities of the staff that is involved in Information Security Management System in relation to the management of Information Security in the Company are the below:

- Applying the Security Policies, related procedures and working instructions that fall within the scope of its work.
- The direct reference to the ISO of any security incident comes to their attention.

8 Policy Approval

The present policy has been approved by the company's Management.