# INFORMATION SECURITY POLICY

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

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

The Security Policy is applied by all staff of the Company involved in the performance of the Services, as well as the equipment used, and the facilities used by the Company in the perfor mance of the Services, including any additional terms of the relevant contracts.

The aim of this policy is to protect the information assets of the Company and its customers from all internal, external, voluntary or involuntary threats.

The individual objectives of the Company regarding Information Security are:

- Information to be protected from unauthorized access
- Ensure the confidentiality of the Information
- Maintain the integrity of the Information
- Maintain the availability of Information
- Ensure compliance with regulatory requirements
- To develop, maintain and test Business Continuity Plans
- Provide Information Security training for all staff
- All actual or suspected safety incidents shall be reported to the ISM and fully investigated

In order to achieve the above objectives, individual Security Policies and Procedures have been developed and implemented, describing the Management's guidelines, the way of implementing the Policy or Process and all relevant staff responsibilities. All staff and external associates (when required), are required to implement Security Policies that fall within the scope of their activities.

The Management is committed to providing all necessary resources for the implementation of this Agreement and the individual Security Policies.

According to the standard framework for the safety of the company's services, the strategic objectives of **CRS LIKNOSS** are defined as:

- High returns on IT-driven business investments
- Information risk management
- Improving the services offered
- Competitive Services
- Ensure continuity and availability of the service.

Information security is **a priority** in order to:

- Ensure full compliance by the company with the relevant legal and regulat ory requirements,
- Protect the interests of the company and those who trade with it and trus t it for the use and movement of their confidential data,
- Ensure the availability, integrity and confidentiality of information generat ed, received and handled in security projects,
- Maximize the reliability of the company's information resources.

The implementation of the ISMS (Information Security Management System) aims to:

- Protect the stored file, the computational resources and the information transmitted to the company services from any threat, internal or external, intentional or accidental,
- Systematic evaluation and evaluation of risks related to information assur ance with a view to their sound and timely management,
- Data archiving, virus and external intrusion prevention, system access con trol, logging of all security incidents and managing unexpected developme nts,
- Continuously inform management and staff on information security issues and hold training seminars for staff,
- Full commitment of the Company Management to the loyal implementati on and continuous improvement of the ISMS, which complies with the requirements of ISO 27001:2022.

The scope of the company's ISMS is:

***DESIGN, DEVELOPMENT, COMMERCE AND SUPPORT OF S/W PRODUCTS – ELECTRONIC MANAGEMENT, DISTRIBUTION AND PROVISION OF SUPPORT SERVICES RELATED TO TOURISM, TRANSPORTATION AND ENTERTAINMENT EVENTS***.

The Information Security Manager is responsible for controlling and monitoring the operatio n of the ISMS, as well as for informing all the staff involved about the Information Security Policy.

All personnel involved in the activities and procedures described and relating to Information Security are responsible for implementing the ISMS's policy and the relevant Procedures and Policies in the field of its work.

Management and all employees are committed to the achievement of the company's objecti ves and to the observance of the principles in relation to Information Security.

Any employee who violates this Security Policy may be liable to disciplinary action at the discretion of the Company Management.

In order to achieve the above, the Company implements an Information Security Manageme nt System according to the ISO / IEC27001:2022 standard.