

Information Security Policy

The protection of information and its processing systems is of strategic importance for the Company in order to achieve its short and long term objectives and at the same time to ensure the confidentiality of the data of the customers receiving its services.

The Company, recognizing the criticality of information and information systems in the execution of its business operations, applies an Information Security Policy with the following Information Security objectives:

- Ensuring the confidentiality, integrity and availability of the information it manages,
- Ensuring the proper functioning of information systems,
- The timely response to incidents that may endanger the Company's business operations,
- Meeting legislative and regulatory requirements,
- The continuous improvement of the level of Information Security.

For this purpose:

- The organisational structures necessary for monitoring issues related to Information Security are defined.
- Technical measures to control and restrict access to information and information systems shall be defined.
- The way in which information is graded according to its importance and value is defined.
- The necessary actions to protect information during the stages of its processing, storage and circulation are described.
- The ways of informing and training the Company's employees and partners on Information Security issues are defined.
- Identify ways to respond to Information Security incidents.
- Describe the ways in which the safe continuity of the Company's business operations is ensured in case of malfunction of information systems or in cases of disasters.

The Company carries out assessments of the risks related to Information Security at regular intervals and takes the necessary measures to address them. It implements a framework for evaluating the effectiveness of its Information Security processes, through which performance indicators are defined, the methodology for measuring them is described and periodic reports are produced and reviewed by the Top Management in order to continuously improve the system.

The CISO is responsible for controlling and monitoring the policies and procedures related to Information Security and taking the necessary initiatives to eliminate all those factors that may compromise the availability, integrity and confidentiality of the Company's information.

All employees of the Company and its partners with access to information and information systems of the Company are responsible for complying with the rules of the applicable Information Security Policy.

The Company is committed to the continuous monitoring and compliance with the regulatory and legislative framework and to the continuous implementation and improvement of the effectiveness of the Information Security Management System.

 Lykourgou 14-16, 10552 Athens, Greece

 +302103249242

 info@everesttravel.gr

 www.everesttravel.gr

Branch Offices Thessaloniki - Salamina

Member of  