

INFORMATION SECURITY POLICY

INFORMATION SECURITY POLICY

The protection of information and its processing systems is of strategic importance for the Company in order to achieve its short-term and long-term goals and simultaneously ensure the confidentiality of the data of clients receiving its services.

Recognizing the criticality of information and information systems in the execution of its business operations, the Company applies an Information Security Policy with the aim of:

- Ensuring the confidentiality, integrity, and availability of information generated, received, and circulated in the context of software development, interconnection, and support services.
- Ensuring proper operation and maximizing the reliability of information systems.
- The timely handling of incidents capable of jeopardizing the Company's business operations.
- Meeting legislative and regulatory requirements.
- Continually improving the level of Information Security.
- Ensuring the provision of software development, interconnection, and support services, consulting services, software development project management, and IT and telecommunications training services.

For this purpose:

- The organizational structures necessary for monitoring matters related to Information Security are defined.
- Technical measures to control and restrict access to information and information systems are defined.
- The method of classifying information according to its importance and value is determined.
- The necessary actions to protect information during the stages of its processing, storage, and circulation are described.
- The methods of informing and training employees and associates of the Company on Information Security issues are specified.
- The methods for handling Information Security incidents are determined.
- The methods by which the secure continuity of the Company's business operations is ensured in cases of information system malfunction or disasters are described.

The Company performs risk assessments related to Information Security at regular intervals and takes the necessary measures to address them. It applies a framework for assessing the effectiveness of Information Security procedures, through which performance indicators are determined, their measurement methodology is described, and periodic reports are generated and reviewed by the Management for continuous system improvement.

The Information Security Officer (CISO) is responsible for auditing and monitoring policies and procedures related to Information Security and taking the necessary initiatives to eliminate all those factors that can endanger 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 bear the responsibility of complying with the rules of the implemented Information Security Policy.



Εγχειρίδιο Ενοποιημένου Συστήματος Διαχείρισης

Εγχ.

The Company commits to the uninterrupted monitoring and observance of the regulatory and legislative framework and to the continuous implementation and improvement of the effectiveness of the Information Security Management System.

For the Management
Antonis Billiris
Chief Executive Officer