

1.5 INFORMATION SECURITY POLICY

Information Security is set as top priority in order to:

- Ensure full business compliance with relevant legal and regulatory requirements
- Protect the interests of the company and those who make deals with and put their trust in it for the use and distribution of their confidential data
- Ensure the availability, integrity and confidentiality of the data produced, received and distributed under security projects
- Maximize reliability of business information resources

The ISMS implementation has the following targets:

- To protect the file kept, computing resources and information distributed at business services from every threat, internal or external, intentional or random
- To systematically assess and evaluate risks concerning information, ensuring their proper and on time management
- Data filing, avoiding viruses and external invasions, access control on systems, recording every information security incident and managing unexpected events
- Continuous updating of the Management and personnel on information security issues, and conducting training seminars for the personnel
- Full commitment of the Management of the company to the strict application and continuous improvement of ISMS, which complies with ISO 27001:2013 standard requirements.

The Chief Information Security Officer has the responsibility to control and monitor the ISMS operation, as well as to update all involved personnel to the Information Security Policy.

All personnel involved in the described activities and procedures concerning Information Security are responsible for the application of the Policy and relevant ISMS Procedures at each labor sector.

The Management and all employees are committed to the achievement of business objectives and to comply with the principles regarding Information Security.

For the achievement of the above, the Company implements an Information Security Management System according to EN ISO 27001:2013 standard.

THE MANAGEMENT

CHRISTOS ZORBAS