

## INFORMATION SECURITY POLICY

VANOS S.A. carries out its activities so as to meet the needs and expectations of its stakeholders in the most effective and safe way, whilst taking into account the applicable standards, legislation, regulations, as well as the instructions for their implementation throughout its activities, while is committed to their observance.

The activities of VANOS S.A. are:

- Trade of General Supplies, Nautical Charts & Publications, Safety Equipment, Personal Protective Equipment and Medical Devices.
- Development and Provision of Training Services, Calibration & Maintenance of Personal Protective Equipment and Safety Equipment, Sales via E-shop.
- Import, Storage, Sales and Distribution of Food Products (Chilled, Frozen and Room Temperature), Beverage and Bonded Stores.

The physical security of the company's facilities, personnel, documents, software and perishable materials is ensured in accordance with the relevant policies and procedures.

All Department Managers are responsible for the appropriate staff training, so that all employees are able to use the company assets allocated to them for performing their work in the safest and most efficient way.

Risk assessment is a repetitive effort and takes into account the contribution of each element to the company's mission, the weaknesses, risks, the consequences of a possible attack, single points of failure, method of quantification and valuation of risks, as well as ways to reduce the impact through the application of protection measures.

Specifications for the procurement of new systems or for the extension of existing systems shall include security requirements appropriate to the task they are or will perform.

Access to the company's LAN, as well as to the devices interconnected to it, is controlled. Access to project software development systems is granted to authorized personnel working on this project.

The company's LAN is being protected by a centrally controlled system from, known or not, harmful software. Files containing the security features against harmful software are updated frequently and automatically. The system protects servers, workstations, as well as remote computers, amongst others. A centrally controlled system protects the internal network from the Internet. The company applies/operates according to a Business Continuity Plan, while also monitoring its applicability.

In conclusion, VANOS S.A. is committed to the continuous improvement of the Information Security Management System according to ISO 27001:2013 Standard's requirements.

Aikaterini D. Vanos  
CEO / President