The protection of the information and processing systems is of strategic importance to the Company in order to achieve its short- and long-term goals and at the same time to ensure the privacy of the customers who receive its services.

SARMED, recognizing the criticality of information and information systems in the performance of its operational functions, implements an Information Security Policy which aims at:

- ensuring the confidentiality, integrity and availability of the information it processes.
- ensuring the correct operation of information systems.
- the timely handling of incidents that may endanger the Company's operations.
- the compliance with legislative and regulatory requirements.
- the continuous improvement of the Information Security level.

For this purpose:

- the organizational units needed to monitor Information Security issues are defined.
- technical measures to control and restrict access to information and information systems are defined.
- how information is classified according to its importance and criticality is determined.
- the necessary steps to protect the information during its processing, storage and transfer phases are described.
- methods of informing and training employees and collaborators of the company on matters of Information Security are defined.
- the ways Information Security incidents are handled, are determined.
- the methods for ensuring the continuous operation of business processes in cases of information systems failures or physical disasters are described.

SARMED conducts Information Security risk assessments periodically and determines the required corrective actions. The Company evaluates the effectiveness of the Information Security procedures by defining performance indicators, describing their measurement methods and producing periodic reports which are being reviewed for continuously improving the ISMS.

The Information Security Officer is responsible for the operation and control of Information Security Policies and Procedures, as well as for taking the required initiatives to eliminate any factor that may lead to company's information availability, integrity or confidentiality compromise.

Company's employees and partners with access to information and information systems are responsible for adhering to the rules of the implemented Information Security Policy.

SARMED is committed to continuously monitor and enforce the regulatory and legislative framework and to continuously implement and improve the effectiveness of the Information Security Management System.

President and CEO of SARMED

Ioannis Sarantitis