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 manages, regardless of its location (on-premise or cloud).
- Ensuring the proper functioning of information systems and services provided
- The timely response to incidents that may jeopardize the company's business operations.
- The satisfaction of legislative and regulatory requirements.
- The continuous improvement of the level of Information Security and data protection mechanisms

For this purpose:

- the organizational units needed to monitor Information Security issues are defined.
- Technical and administrative measures are defined for access to information and systems located in the cloud, ensuring that cloud service providers meet the necessary security standards.
- 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 risk assessments related to Information Security and cloud infrastructure in order to identify new threats and take appropriate countermeasures at regular intervals. 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.

All employees of the Company and its partners with access to the Company's information and information systems, including cloud services, are responsible for complying with the rules of the applicable 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.

Chairman and CEO of SARMED

Ioannis Sarantitis