CORPORATE INFORMATION SECURITY POLICY

ESS conducts each of its activities in such a way, to serve the needs and expectations of its customers in the most efficient and secure manner and takes into account the applicable standards, legislation, regulations, as well as their application guidelines in all its activities and undertakes to comply with them.

The activities of ESS are:

- *Design, Development, Testing and Characterization of MEMS Sensor Dies*
- *Design, Development, Production, Testing and Characterization of Sensor Systems*
- *Feasibility Studies and Prototyping of MEMS based Sensor Systems*
- *Scientific and Technical Consulting, Analysis and Testing of Sensors and Sensor Systems*
- *Assembly, Integration and Verification of Printed Circuits Boards*
- *Design, Development and Installation of Integrated IoT Solutions*
- *Scientific and Technical consulting for IoT Systems*

The physical security of facilities, personnel, documents, software and vulnerable equipment is ensured by the company in accordance with the relevant policies and procedures.

The heads of the Departments are responsible for the appropriate training of the staff so that they are able to use in the safest and most efficient way the assets of the company available to them to carry out their work.

Risk assessment is an iterative effort and considers each component's contribution to the company's mission, vulnerabilities, risks, impact of a potential breach, single points of failure, method of quantifying and assessing risks, and ways to mitigate impacts through implementation protection measures.

The specifications for the supply of new or for the expansion of existing systems also include security requirements depending on the mission they perform or are about to perform.

Access to the corporate network, as well as to the devices interconnected to it, is controlled. Access to the company's support systems is given to authorised personnel working for this purpose.

A centrally controlled system protects the corporate network from known or unknown malicious software. The files containing the anti-malware features are updated frequently and automatically. The system protects, among other things, servers, workstations, and remote computers. A centrally controlled system protects the internal network from the Internet. The company has a Business Continuity Plan and maintains its applicability.

Finally, the company is committed to the continuous improvement of the Information Security Management System according to the last version of ISO 27001 with which it complies and to achieve the Information Security objectives.

Athens, 08 October 2024

CEO
E. Karampoikis