INFORMATION SECURITY POLICY

ESS conducts all of its activities in order to meet the needs and expectations of its customers in the most effective and secure manner, taking into account applicable standards, legislation, regulations, as well as their implementation guidelines in all of its operations, and is committed to their compliance.

The activities of ESS include:

- ***Design, Development, Testing and Characterization of Microelectronic Sensors (MEMS)***
- ***Design, Development, Production, Testing and Characterization of Sensor Systems***
- ***Feasibility Study and Construction of Prototype Sensor Systems based on Microelectronic Sensors (MEMS)***
- ***Provision of Scientific and Technical Consulting, Analyses and Testing of Sensors and Sensor Systems***
- ***Development and Installation of Integrated Information and Telecommunication Solutions for the Internet of Things (IoT)***
- ***Provision of related Scientific and Technical Consulting for the Internet of Things (IoT)***
- ***Assembly, Integration and Verification of Printed Circuit Boards***

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

Department Heads are responsible for the appropriate training of personnel so that they can use, in the safest and most efficient way, the company's assets made available to them for the performance of their duties. The company ensures the continuous awareness and training of personnel on issues of information security, data protection, and security incident management.

Risk assessment is a recurring effort that takes into account the contribution of each element to the company's mission, weaknesses, risks, impacts from potential incidents, single points of failure, methods of quantifying and evaluating risks, as well as measures to reduce impacts through the implementation of protection controls. The results of risk assessments are periodically evaluated and form the basis for decisions regarding the implementation and improvement of security controls.

Specifications for the procurement of new systems or the expansion of existing ones include security requirements appropriate to the mission they perform or are intended to perform.

Access to the corporate network and to connected devices is controlled. Access to the company's support systems is granted only to authorized personnel working for that purpose.

A centrally managed system protects the corporate network from known or unknown malicious software. The files containing malware protection signatures are updated frequently and automatically. The system protects, among others, servers, workstations, and remote computers. A centrally managed system also protects the internal network from the Internet.

ES SYSTEMS
Sensors • IoT

The company maintains a Business Continuity Plan and ensures its operability. In addition, it maintains a procedure for reporting, investigating, and managing information security incidents to ensure prompt response and mitigation of potential impacts.

Finally, the company is committed to the continual improvement of its Information Security Management System, in accordance with the latest version of **ISO 27001:2022**, with which it complies, and to achieving its Information Security objectives.

The company's Management reviews this Policy at regular intervals to ensure its continuing suitability, adequacy, and effectiveness.

Athens, October 10, 2025

CEO

E. Karampoikis

ΕΤΑΙΡΙΚΗ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Η ESS διενεργεί κάθε δραστηριότητά της έτσι ώστε να εξυπηρετεί τις ανάγκες και τις προσδοκίες των πελατών της με τον πιο αποτελεσματικό και ασφαλή τρόπο και λαμβάνει υπόψη της τα ισχύοντα πρότυπα, τη νομοθεσία, τους κανονισμούς, καθώς και τις οδηγίες εφαρμογής τους σε όλες τις δραστηριότητές της και δεσμεύεται για την τήρησή τους.

Οι δραστηριότητες της ESS είναι:

- ***Σχεδιασμός, Ανάπτυξη, Έλεγχος και Χαρακτηρισμός Αισθητήρων Μικροηλεκτρονικής (MEMS)***
- ***Σχεδιασμός, Ανάπτυξη, Παραγωγή, Έλεγχος και Χαρακτηρισμός Συστημάτων Αισθητήρων***
- ***Μελέτη Σκοπιμότητας και Κατασκευή Πρωτότυπων Συστημάτων Αισθητήρων βασισμένων σε Αισθητήρες Μικροηλεκτρονικής (MEMS)***
- ***Παροχή Επιστημονικών και Τεχνικών Συμβουλών, Αναλύσεις και Δοκιμές Αισθητήρων και Συστημάτων Αισθητήρων***
- ***Ανάπτυξη και Εγκατάσταση Ολοκληρωμένων Λύσεων Πληροφορικής και Τηλεπικοινωνιών για το Διαδίκτυο Πραγμάτων (Internet of Things)***
- ***Παροχή σχετικών Επιστημονικών και Τεχνικών Συμβουλών για το Διαδίκτυο Πραγμάτων (Internet of Things)***
- ***Συναρμολόγηση, Ολοκλήρωση και Επαλήθευση Πινακίδων Τυπωμένων Κυκλωμάτων***

Η φυσική ασφάλεια των εγκαταστάσεων, του προσωπικού, των εγγράφων, των λογισμικών και του ευπαθούς εξοπλισμού εξασφαλίζεται από την εταιρεία σύμφωνα με τις σχετικές πολιτικές και διαδικασίες.

Οι υπεύθυνοι των Τμημάτων είναι αρμόδιοι για την κατάλληλη εκπαίδευση του προσωπικού ώστε να είναι σε θέση να χρησιμοποιούν με τον ασφαλέστερο και αποδοτικότερο τρόπο τα περιουσιακά στοιχεία της εταιρείας που τους διατίθενται για τη διεκπεραίωση της εργασίας τους. Η εταιρεία μεριμνά για τη συνεχή ευαισθητοποίηση και εκπαίδευση του προσωπικού σε θέματα ασφάλειας πληροφοριών, προστασίας δεδομένων και διαχείρισης περιστατικών ασφάλειας.

Η αποτίμηση των κινδύνων είναι επαναλαμβανόμενη προσπάθεια και λαμβάνει υπόψη τη συμβολή κάθε στοιχείου στην αποστολή της εταιρείας, τις αδυναμίες, τους κινδύνους, τις επιπτώσεις από ενδεχόμενη προσβολή, μοναδικά σημεία αστοχίας, μέθοδο ποσοτικοποίησης και αποτίμησης των κινδύνων, καθώς και τρόπους μείωσης των επιπτώσεων μέσω εφαρμογής μέτρων προστασίας. Τα αποτελέσματα των εκτιμήσεων κινδύνου αξιολογούνται περιοδικά και αποτελούν τη βάση για τη λήψη αποφάσεων σχετικά με την εφαρμογή και βελτίωση των ελέγχων ασφάλειας.

Οι προδιαγραφές για την προμήθεια νέων ή για την επέκταση υπαρχόντων συστημάτων περιλαμβάνουν και απαιτήσεις ασφαλείας ανάλογα με την αποστολή την οποία επιτελούν ή πρόκειται να επιτελέσουν.

Η πρόσβαση στο εταιρικό δίκτυο, καθώς και στις συσκευές που είναι διασυνδεδεμένες προς αυτό, είναι ελεγχόμενη. Πρόσβαση στα συστήματα υποστήριξης της εταιρείας έχει μόνο το εξουσιοδοτημένο προσωπικό που εργάζεται για τον σκοπό αυτό.

Ένα κεντρικά ελεγχόμενο σύστημα προστατεύει το εταιρικό δίκτυο από γνωστό ή άγνωστο επιβλαβές λογισμικό. Τα αρχεία που περιέχουν τα χαρακτηριστικά ασφάλειας έναντι του επιβλαβούς λογισμικού ενημερώνονται συχνά και αυτόματα. Το σύστημα προστατεύει μεταξύ άλλων τους servers, τους σταθμούς εργασίας, καθώς και τους απομακρυσμένους υπολογιστές. Ένα κεντρικά ελεγχόμενο σύστημα προστατεύει το εσωτερικό δίκτυο από το Internet.

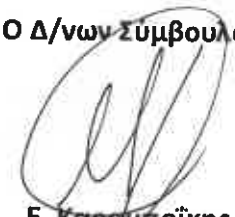
Η εταιρεία διαθέτει Σχέδιο Επιχειρηματικής Συνέχειας και συντηρεί τη δυνατότητα εφαρμογής του. Επιπλέον, διατηρεί διαδικασία αναφοράς, διερεύνησης και διαχείρισης περιστατικών ασφάλειας πληροφοριών, ώστε να εξασφαλίζεται η άμεση αντιμετώπιση και αποκατάσταση πιθανών επιπτώσεων.

Τέλος, η εταιρεία δεσμεύεται για τη διαρκή βελτίωση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών βάσει της τελευταίας έκδοσης του **ISO 27001:2022**, με το οποίο και συμμορφώνεται, και για την επίτευξη των στόχων Ασφάλειας Πληροφοριών.

Η Διοίκηση της εταιρείας επανεξετάζει σε τακτά χρονικά διαστήματα την παρούσα πολιτική, ώστε να διασφαλίζεται η συνεχιζόμενη καταλληλότητα, επάρκεια και αποτελεσματικότητά της.

Αθήνα, 10 Οκτωβρίου 2025

Ο Δ/νων Σύμβουλος



Ε. Καραμπογιάκης