# ΕΤΑΙΡΙΚΗ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Η NEOKEM 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 δραστηριότητές της και δεσμεύεται για την τήρησή τους.

Οι δραστηριότητες της NEOKEM, είναι:
Σχεδιασμός, Ανάπτυξη, Παραγωγή, Διάθεση και Παροχή Υπηρεσιών Υποστήριξης σε Χρώματα Πούδρας, Βιομηχανικά Χρώματα, Ναυτιλιακά Χρώματα, Οικοδομικά Χρώματα και Κόλλες για Βιομηχανική και Ναυτιλιακή Χρήση.

Η παρούσα πολιτική είναι ευθυγραμμισμένη με την Επιχειρηματική Στρατηγική και τις σχετικές απαιτήσεις της Εταιρείας. Ως Ασφάλεια Πληροφοριών ορίζεται η προστασία της Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας των Πληροφοριών. Η φυσική ασφάλεια των εγκαταστάσεων, προσωπικού, εγγράφων, λογισμικών και 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 την διεκπεραίωση της εργασίας τους.

Η αποτίμηση των κινδύνων είναι επαναλαμβανόμενη προσπάθεια και λαμβάνει υπόψη την 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.

Οι προδιαγραφές για την προμήθεια νέων ή για την επέκταση υπαρχόντων συστημάτων, περιλαμβάνουν και απαιτήσεις ασφαλείας ανάλογα με την αποστολή την οποία επιτελούν η πρόκειται να επιτελέσουν. Η πρόσβαση στο εταιρικό δίκτυο, καθώς στις συσκευές που είναι διασυνδεδεμένες προς αυτό είναι ελεγχόμενη. Πρόσβαση στα συστήματα υποστήριξης της εταιρείας έχει το εξουσιοδοτημένο προσωπικό που εργάζεται για το 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 την δυνατότητα εφαρμογής του.

Τέλος, η εταιρεία δεσμεύεται για την διαρκή βελτίωση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών κατά ISO 27001:2022 με το οποίο συμμορφώνεται και την επίτευξη των στόχων Ασφάλειας Πληροφοριών που θέτει, μέσω του πλαισίου της παρούσας πολιτικής, καθώς και των επιμέρους πολιτικών και διαδικασιών που εφαρμόζονται για το σκοπό αυτό.

Η παρούσα πολιτική ανασκοπείται ετήσια ή οποτεδήποτε υπάρχουν σημαντικές αλλαγές και είναι διαθέσιμη σε όλα τα ενδιαφερόμενα μέρη.

# CORPORATE INFORMATION SECURITY POLICY

NEOKEM 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 considers the applicable standards, legislation, regulations, as well as their application guidelines in all its activities and undertakes to comply with them.

The activities of NEOKEM are:
Design, Development, Production, Distribution and Servicing of Powder Coatings, Industrial Coatings, Marine Paints, Decorative Paints and Glues for Industrial and Marine Use.

This policy is aligned with the Business Strategy and the relevant requirements of the Company. Information Security is defined as the protection of Confidentiality, Integrity and Availability of Information 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 ISO 27001:2022 with which it complies and the achievement of the Information Security objectives it sets, through the framework of this policy, as well as the individual policies and procedures applied for this purpose.

This policy is reviewed annually or whenever there are significant changes and is available to all interested parties.

Αθήνα, 02 Σεπτεμβρίου 2024 | Athens, 02 September 2024
CEO Γ. Βλαχάκης | G. Vlahakis