

## ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Η **SIGMA SOFT** ανταποκρινόμενη στις απαιτήσεις της σύγχρονης επιχειρηματικής πραγματικότητας και στοχεύοντας στην προστασία των πληροφοριακών συστημάτων που χρησιμοποιεί και αναπτύσσει καθώς και των πληροφοριών που διαχειρίζεται, συμπεριλαμβανομένων και των προσωπικών πληροφοριών υγείας, μέσω πρόσβασης κατά την υποστήριξη των πελατών, αποφάσισε να σχεδιάσει και να εγκαταστήσει ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών σύμφωνα με τις απαιτήσεις του Διεθνούς Προτύπου **ISO 27001:2013** με παράλληλη κάλυψη απαιτήσεων του προτύπου **ISO 27799:2016** αναφορικά με την προστασία των προσωπικών πληροφοριών υγείας.

Το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών της Εταιρείας καλύπτει τον Σχεδιασμό, Ανάπτυξη, Εγκατάσταση και Υποστήριξη Λογισμικού & την Εμπορία Hardware και σχεδιάστηκε σύμφωνα με τις ανάγκες και τις επιδιώξεις της Εταιρείας και τις Νομικές και Κανονιστικές Απαιτήσεις της ισχύουσας Ελληνικής και Κοινοτικής Νομοθεσίας.

Οι βασικοί στόχοι, έτσι όπως αυτοί εκφράζονται μέσα στις διαδικασίες του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών της εταιρίας, είναι:

- η δημιουργία βάσης για τη διαρκή βελτίωση της αποτελεσματικότητας των διεργασιών της, έχοντας ως γνώμονα τη συνεχή ικανοποίηση των αναγκών και των προσδοκιών των πελατών της στο μέγιστο δυνατό βαθμό.
- η ελαχιστοποίηση του αριθμού των συμβάντων που μπορεί να επηρεάσουν τη συνέχεια των επιχειρησιακών διεργασιών, καθώς και την κατά το δυνατόν μείωση των επιπτώσεών τους.
- ο χειρισμός των πληροφοριών, που τηρούνται και διακινούνται με οποιονδήποτε τρόπο μέσα από τα ηλεκτρονικά και μη συστήματα της και αποτελούν στοιχεία εξαιρετικής σημασίας για τη λειτουργία και τη θέση της στην αγορά, με τρόπο που προστατεύει την ασφάλειά τους ως προς την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους,
- η ασφάλεια των προσωπικών πληροφοριών υγείας από άποψη εμπιστευτικότητας, διαθεσιμότητας αλλά και ακεραιότητας, στις οποίες έχει πρόσβαση η εταιρία μέσω της υποστήριξης των μηχανογραφικών συστημάτων των πελατών της
- η συμμόρφωση με τους νόμους και τις κανονιστικές διατάξεις στις οποίες υπόκειται η εταιρία για την ανάπτυξη & υποστήριξη των μηχανογραφικών εφαρμογών αλλά και για την διαχείριση προσωπικών πληροφοριών υγείας

Στόχος της Διοίκησης αναφορικά με την προστασία των προσωπικών δεδομένων και ιδίως των προσωπικών δεδομένων υγείας είναι η συμμόρφωσή της με τις παρακάτω αρχές:

- Επεξεργασία των προσωπικών δεδομένων & δεδομένων υγείας με τρόπο θεμιτό και νόμιμο
- Τήρηση των προσωπικών δεδομένων & δεδομένων υγείας για σαφώς καθορισμένους σκοπούς
- Περιορισμός των προσωπικών δεδομένων & δεδομένων υγείας στα απολύτως απαραίτητα για την επίτευξη των σκοπών αυτών
- Προστασία των προσωπικών δεδομένων & δεδομένων υγείας μέσω επαρκών μέτρων ασφάλειας
- Τήρηση των προσωπικών δεδομένων & δεδομένων υγείας για ορισμένο χρονικό διάστημα (ανάλογα με τους σκοπούς).

Το σύστημα της εταιρίας ανασκοπείται σε τακτά χρονικά διαστήματα από τη Διοίκηση, προκειμένου να προσαρμόζεται στις νέες ανάγκες και εξελίξεις της αγοράς, στις νομοθετικές απαιτήσεις, αλλά και στην επίτευξη του στόχου για την ασφάλεια της πληροφορίας της εταιρίας. Σε ετήσια βάση ανασκοπούνται και οι στόχοι για την Ασφάλεια Πληροφοριών και εφόσον απαιτείται αναπροσαρμόζονται.

Η Διοίκηση δεσμεύεται στη διάθεση της υποδομής και του εξοπλισμού που κρίνεται απαραίτητη για την υλοποίηση και διαθεσιμότητα των εργασιών της. Κάθε εργαζόμενος είναι υπεύθυνος να ανταποκρίνεται, να αφομοιώνει και να εφαρμόζει τις διαδικασίες που απαιτεί το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών μέσα από τις καθημερινές δραστηριότητές του. Για το λόγο αυτό όλοι οι εργαζόμενοι, ανάλογα με τις αρμοδιότητές τους, ενημερώνονται σχετικά με το Σύστημα και ενεργούν αποδεδειγμένα σύμφωνα με τους καθορισμένους κανόνες ασφάλειας και εμπιστευτικότητας.

Η Πολιτική Ασφάλειας Πληροφοριών είναι κοινοποιημένη, κατανοητή και εφαρμόσιμη από το σύνολο του ανθρώπινου δυναμικού, με απώτερο σκοπό τη συνεχή, σταθερή ανάπτυξη της επιχειρηματικής δραστηριότητάς της, με αταλάντευτη προσήλωση στις αρχές της και τη διαρκή προσφορά στους πελάτες της προϊόντων και υπηρεσιών αρίστης ποιότητας. Ανασκοπείται σε τακτά χρονικά διαστήματα με στόχο τη συνεχή εναρμόνισή της με τις συνθήκες της αγοράς, τις τεχνολογικές εξελίξεις και την κείμενη νομοθεσία.

Διαδικασίες, ροές και ενέργειες, οι οποίες δεν εγγυώνται την εκπλήρωση των στόχων που έχουν τεθεί, διακόπτονται άμεσα από τους υπεύθυνους, διεξάγονται αναλύσεις αιτιών και ορίζονται τα απαιτούμενα μέτρα βελτίωσης.

### **Διευθύνων Σύμβουλος**

Στεφανίδης Γεώργιος

Θεσσαλονίκη, 03/09/2018

(Έκδοση: 1)