ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Η UCANDRONE αναγνωρίζει ότι οι πληροφορίες, τα πληροφοριακά συστήματα, οι τεχνολογικές υποδομές, η πνευματική ιδιοκτησία, τα δεδομένα έρευνας και ανάπτυξης, τα δεδομένα παραγωγής, καθώς και οι πληροφορίες πελατών, συνεργατών και προμηθευτών αποτελούν κρίσιμα περιουσιακά στοιχεία της εταιρείας. Για τον λόγο αυτό δεσμεύεται να διασφαλίζει τη διαθεσιμότητα, την ακεραιότητα και την εμπιστευτικότητα των πληροφοριών που δημιουργεί, επεξεργάζεται, αποθηκεύει, διαβιβάζει και διαχειρίζεται, προστατεύοντάς τες από κάθε μορφή απειλής, είτε αυτή είναι εσωτερική είτε εξωτερική, σκόπιμη ή τυχαία.

Η παρούσα Πολιτική Ασφάλειας Πληροφοριών καθορίζει τις βασικές αρχές και τις δεσμεύσεις της εταιρείας για την ανάπτυξη, εφαρμογή, λειτουργία, παρακολούθηση και συνεχή βελτίωση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, σύμφωνα με τις απαιτήσεις του προτύπου ISO/IEC 27001, τις ισχύουσες νομοθετικές και κανονιστικές απαιτήσεις, τις συμβατικές υποχρεώσεις της εταιρείας, καθώς και τις αρχές της κυβερνοασφάλειας και της διαχείρισης κινδύνων.

Δέσμευση της Διοίκησης και Αντικειμενικοί Σκοποί και Στόχοι

Η Διοίκηση της UCANDRONE θεωρεί ότι η ασφάλεια πληροφοριών αποτελεί αναπόσπαστο μέρος της επιχειρησιακής λειτουργίας, της έρευνας και ανάπτυξης, της σχεδίασης, της παραγωγής, της υποστήριξης πελατών και της συνεχούς επιχειρησιακής ανάπτυξης της εταιρείας και δεσμεύεται για την ενσωμάτωσή της σε όλες τις επιχειρησιακές διεργασίες.

Για την επίτευξη των παραπάνω, η εταιρεία δεσμεύεται να:

- Προστατεύει όλα τα πληροφοριακά περιουσιακά στοιχεία από μη εξουσιοδοτημένη πρόσβαση, αποκάλυψη, αλλοίωση, απώλεια ή καταστροφή.
- Διασφαλίζει την εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα, αυθεντικότητα και ιχνηλασιμότητα των πληροφοριών καθ' όλη τη διάρκεια του κύκλου ζωής τους.
- Προστατεύει τα προσωπικά δεδομένα, τα εμπορικά δεδομένα, τα τεχνικά αρχεία, τα σχέδια, τον πηγαίο κώδικα λογισμικού, τα δεδομένα έρευνας και ανάπτυξης, τις πληροφορίες παραγωγής και κάθε μορφή πνευματικής ιδιοκτησίας.
- Διασφαλίζει την ασφαλή λειτουργία των πληροφοριακών συστημάτων, των δικτύων, των υπολογιστικών υποδομών, των εφαρμογών και των υπηρεσιών πληροφορικής.
- Αναγνωρίζει, αξιολογεί και αντιμετωπίζει συστηματικά τους κινδύνους που σχετίζονται με την ασφάλεια πληροφοριών μέσω τεκμηριωμένης διαδικασίας διαχείρισης κινδύνων.
- Εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας ανάλογα με την κρισιμότητα και την ευαισθησία κάθε πληροφοριακού πόρου.
- Συμμορφώνεται με όλες τις εφαρμοστέες νομοθετικές, κανονιστικές και συμβατικές απαιτήσεις που σχετίζονται με την ασφάλεια πληροφοριών, την κυβερνοασφάλεια, την προστασία προσωπικών δεδομένων και τις απαιτήσεις των πελατών.

- Ενισχύει την ανθεκτικότητα της εταιρείας απέναντι σε κυβερνοεπιθέσεις, κακόβουλο λογισμικό, περιστατικά παραβίασης πληροφοριών, τεχνικές βλάβες και κάθε άλλη απειλή που ενδέχεται να επηρεάσει τη λειτουργία της.
- Υποστηρίζει την επιχειρησιακή συνέχεια μέσω της προστασίας κρίσιμων πληροφοριακών πόρων και της αποτελεσματικής διαχείρισης περιστατικών ασφάλειας πληροφοριών.
- Προωθεί την κουλτούρα ασφάλειας πληροφοριών σε όλα τα επίπεδα της εταιρείας.

Για την επίτευξη των στόχων αυτών η UCANDRONE:

- Εφαρμόζει και βελτιώνει διαρκώς Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών σύμφωνα με το ISO/IEC 27001.
- Θέτει μετρήσιμους στόχους ασφάλειας πληροφοριών, οι οποίοι παρακολουθούνται, αξιολογούνται και ανασκοπούνται σε τακτική βάση.
- Παρέχει τους απαραίτητους ανθρώπινους, οικονομικούς, τεχνολογικούς και οργανωτικούς πόρους για την αποτελεσματική λειτουργία του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.
- Εφαρμόζει πολιτικές και διαδικασίες για τη διαχείριση πρόσβασης, την κρυπτογράφηση, τη δημιουργία αντιγράφων ασφαλείας, την καταγραφή συμβάντων, τη διαχείριση ευπαθειών, την ασφαλή διαχείριση αλλαγών και την προστασία των πληροφοριακών συστημάτων.
- Διασφαλίζει ότι όλα τα περιστατικά ασφάλειας πληροφοριών αναφέρονται, αξιολογούνται, αντιμετωπίζονται και διερευνώνται με οργανωμένο τρόπο, ώστε να αποτρέπεται η επανάληψή τους.
- Διενεργεί τακτικές αξιολογήσεις κινδύνων, εσωτερικούς ελέγχους, δοκιμές και ανασκοπήσεις της Διοίκησης για την αξιολόγηση της αποτελεσματικότητας του Συστήματος.
- Εφαρμόζει κατάλληλα μέτρα για την ασφαλή συνεργασία με προμηθευτές, συνεργάτες και τρίτα μέρη που έχουν πρόσβαση σε πληροφορίες ή πληροφοριακά συστήματα της εταιρείας.
- Προάγει τη συνεχή ενημέρωση, εκπαίδευση και ευαισθητοποίηση του προσωπικού σε θέματα ασφάλειας πληροφοριών και κυβερνοασφάλειας.
- Ενσωματώνει τις απαιτήσεις ασφάλειας πληροφοριών στον σχεδιασμό νέων έργων, προϊόντων, υπηρεσιών και τεχνολογικών λύσεων, εφαρμόζοντας τις αρχές της ασφάλειας εξ αρχής (Security by Design) και της ελαχιστοποίησης του κινδύνου.

Η Διοίκηση της εταιρείας δεσμεύεται να υποστηρίζει ενεργά την εφαρμογή του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών και Κυβερνοασφάλειας, να εξασφαλίζει τη συνεχή βελτίωσή του και να προωθεί μια κουλτούρα υπευθυνότητας και ασφάλειας σε όλα τα επίπεδα της εταιρείας.

Επίσης, καθορίζει και παρακολουθεί αντικειμενικούς σκοπούς και στόχους για την ασφάλεια των δικτύων και πληροφοριακών συστημάτων, οι οποίοι είναι ευθυγραμμισμένοι με τη στρατηγική, τους επιχειρησιακούς στόχους και τις ανάγκες ανθεκτικότητας της εταιρείας. Οι στόχοι αυτοί ανασκοπούνται ετησίως και επικαιροποιούνται όταν μεταβάλλονται οι κίνδυνοι, οι τεχνολογίες, οι επιχειρησιακές απαιτήσεις ή το κανονιστικό πλαίσιο.

Παρακολούθηση και Ανασκόπηση

Η παρούσα Πολιτική ανασκοπείται τουλάχιστον εξαμηνιαία ή όταν προκύπτουν σημαντικές αλλαγές στις δραστηριότητες, στους κινδύνους, στις τεχνολογίες ή στις νομοθετικές και κανονιστικές απαιτήσεις, ώστε να διασφαλίζεται η συνεχής καταλληλότητα, επάρκεια και αποτελεσματικότητά της.

Ρόλοι και Αρμοδιότητες

Η Διοίκηση διασφαλίζει ότι καθορίζονται, εγκρίνονται και γνωστοποιούνται οι ρόλοι, οι αρμοδιότητες και οι εξουσιοδοτήσεις που σχετίζονται με την ασφάλεια δικτύων και πληροφοριακών συστημάτων.

Ο CISO είναι υπεύθυνος για τον συντονισμό του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, την παρακολούθηση των κυβερνοκινδύνων, την εισήγηση μέτρων προστασίας, τον συντονισμό της αντιμετώπισης περιστατικών κυβερνοασφάλειας και την υποβολή σχετικών αναφορών στη Διοίκηση.

Ο IMS Manager συντονίζει την εφαρμογή του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, παρακολουθεί τη συμμόρφωση με τις πολιτικές και διαδικασίες και υποστηρίζει τις εσωτερικές επιθεωρήσεις και τις ανασκοπήσεις από τη Διοίκηση.

Οι Υπεύθυνοι Τμημάτων εφαρμόζουν τις απαιτήσεις της πολιτικής στις περιοχές ευθύνης τους, ενώ όλοι οι εργαζόμενοι και οι εξωτερικοί συνεργάτες οφείλουν να προστατεύουν τα πληροφοριακά περιουσιακά στοιχεία και να αναφέρουν άμεσα οποιοδήποτε πραγματικό ή ύποπτο περιστατικό ασφάλειας πληροφοριών.

Παρακολούθηση της Αποτελεσματικότητας

Η εφαρμογή της παρούσας Πολιτικής παρακολουθείται μέσω κατάλληλων δεικτών απόδοσης και αποτελεσματικότητας (KPIs), οι οποίοι ανασκοπούνται τουλάχιστον εξαμηνιαία ή κάθε φορά που κρίνεται απαραίτητο από τη Διοίκηση.

Διατήρηση Τεκμηριωμένων Πληροφοριών

Η τεκμηρίωση που σχετίζεται με την εφαρμογή της παρούσας Πολιτικής, τηρείται σύμφωνα με τη διαδικασία ελέγχου τεκμηριωμένης πληροφορίας και το εγκεκριμένο πρόγραμμα χρόνων διατήρησης αρχείων της εταιρείας.

Ενημέρωση και Επικοινωνία

Η συμμόρφωση με την παρούσα Πολιτική αποτελεί υποχρέωση όλων των εργαζομένων, στελεχών, εξωτερικών συνεργατών, προμηθευτών και κάθε τρίτου που αποκτά πρόσβαση σε πληροφορίες ή πληροφοριακά συστήματα της UCANDRONE. Όλοι οφείλουν να εφαρμόζουν τις καθορισμένες πολιτικές και διαδικασίες, να προστατεύουν τα πληροφοριακά περιουσιακά στοιχεία της εταιρείας και να αναφέρουν άμεσα οποιοδήποτε πραγματικό ή ύποπτο περιστατικό ασφάλειας πληροφοριών.

Η Διοίκηση
(Σφραγίδα / Υπογραφή)

UCANDRONE A.E.
ΥΠΗΡΕΣΙΕΣ ΠΕΡΙΒΑΛΛΟΝΤΟΣ & ΠΡΑΣΙΝΟΥ
ΧΑΡΤΟΓΡΑΦΗΣΗ ΤΗΛΕΠΙΣΚΟΠΗΣΗ ΣΧΕΔΙΑΣΜΟΣ
ΑΝΑΠΤΥΞΗ ΜΗ ΕΠΑΝΔΡΩΜΕΝΩΝ ΣΥΣΤΗΜΑΤΩΝ
2ο ΧΛΜ ΛΕΩΦ. ΠΑΛΑΝΙΑΣ - ΜΑΡΚΟΠΟΥΛΟΥ 19440 ΚΟΡΩΠΙ
ΑΦΜ: 800662243 - ΔΟΥ: ΚΕΦΟΔΕ ΑΤΤΙΚΗΣ
ΤΗΛ.: 2130356684-5 - www.ucandrone.com

Ημερομηνία: 17/02/2026