Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων ΛΑΝΑΚΑΜ Α.Ε.

Αριθμός ΓΕΜΗ: 000232901000

Α.Φ.Μ.: 094007209

ΕΙΣΑΓΩΓΗ

Η Πολιτική Ασφάλειας Πληροφοριών και Δεδομένων καταγράφει τη θέση της Διοίκησης αναφορικά με τη στρατηγική που ακολουθεί για την ασφάλεια των πληροφοριών της και καλύπτει όλες τις ενέργειες που πρέπει να γίνονται ώστε να δημιουργηθεί ένα ασφαλές περιβάλλον λειτουργίας. Η άποψη της Διοίκησης για την ασφάλεια των πληροφοριών και η δέσμευσή της ως προς αυτή πρέπει να γίνει κατανοητή σε όλο το προσωπικό της εταιρείας. Η παρούσα Πολιτική Ασφάλειας Πληροφοριών αποτελεί μια περίληψη των βασικότερων μέτρων, τα οποία πρέπει να τηρούνται από όλο το προσωπικό της.

ΣΚΟΠΟΣ ΠΟΛΙΤΙΚΗΣ

Με την παρούσα Πολιτική Ασφάλειας Πληροφοριών η Διοίκηση της δείχνει ρητά τη βούλησή της για τη διασφάλιση των πληροφοριών και των πληροφοριακών πόρων που υποστηρίζουν τις δραστηριότητές της και παρέχει τις κύριες κατευθύνσεις για τη διαχείριση της ασφάλειας των πληροφοριών.

ΣΤΟΙΧΟΙ ΠΟΛΙΤΙΚΗΣ

Πρωταρχικοί Στόχοι της **Πολιτικής Ασφάλειας** είναι:

- Η διασφάλιση της εμπιστευτικότητας, διαθεσιμότητας και ακεραιότητας των πληροφοριών που διαχειρίζεται η εταιρεία.
- Ο έγκαιρος εντοπισμός κινδύνων Ασφάλειας Πληροφοριών και η αποτελεσματική αντιμετώπισή τους.
- Η άμεση αντιμετώπιση περιστατικών Ασφάλειας Πληροφοριών.
- Η διασφάλιση της ομαλής λειτουργίας των πληροφοριακών πόρων.
- Η συνεχής βελτίωση του επιπέδου Ασφάλειας Πληροφοριών.

ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η Πολιτική Ασφάλειας απευθύνεται σε όλο το προσωπικό και στους συνεργάτες οι οποίοι αποκτούν πρόσβαση στα συστήματα, στις πληροφορίες, στις υπηρεσίες και στις εγκαταστάσεις της.

ΓΕΝΙΚΕΣ ΑΡΧΕΣ

Καθορισμός Ιδιοκτητών Πληροφοριών

Κάθε πληροφοριακός πόρος που διαθέτει η εταιρεία και υποστηρίζει συγκεκριμένες επιχειρηματικές λειτουργίες, ανήκει σε έναν (και σε ορισμένες περιπτώσεις περισσότερους) καθορισμένο Ιδιοκτήτη Πληροφοριών ή αλλιώς χρήστες. Ο Ιδιοκτήτης Πληροφοριών φέρει τη συνολική ευθύνη για την προστασία των πληροφοριών που έχει υπό την κατοχή του και σε περίπτωση που μεταβιβάσει κάποιες από τις πληροφορίες σε τρίτους, η συνολική ευθύνη εξακολουθεί και παραμένει σε αυτόν.

Διαβάθμιση Πληροφοριών

Όλες οι πληροφορίες που ανήκουν στην εταιρεία πρέπει να κατηγοριοποιούνται κατάλληλα από τους αντίστοιχους Ιδιοκτήτες Πληροφοριών ανάλογα με το βαθμό κρισιμότητάς τους και το Σχήμα Διαβάθμισης Πληροφοριών.

Διαχείριση Κινδύνων

Η εταιρεία μέσω του Υπευθύνου Διαχείρισης Κινδύνων διενεργεί αποτίμηση των κινδύνων της ασφάλειας πληροφοριών μια φορά το χρόνο κατά ελάχιστο οι οποίες και συμπεριλαμβάνονται στον πίνακα κινδύνων (Risk Matrix) Μέσω της διαδικασίας αυτής ο οργανισμός είναι σε θέση να αναγνωρίζει και να εξετάζει τις αδυναμίες, τις πιθανές απειλές προς τους πόρους της, την πιθανότητα εκδήλωσής τους και κατά συνέπεια τον κίνδυνο που διατρέχουν.

Καταγραφή Εξοπλισμού

Η εταιρεία διατηρεί έναν ενημερωμένο κατάλογο με το πληροφοριακό και δικτυακό εξοπλισμό που στηρίζει την επιχειρηματική λειτουργία του Οργανισμού, το βαθμό κρισιμότητας του αλλά και τον αντίστοιχο Ιδιοκτήτη Πληροφοριών. Οι πόροι που καταγράφονται κατά ελάχιστο είναι οι ακόλουθοι:

- Πληροφοριακοί Πόροι: βάσεις δεδομένων, αρχεία δεδομένων, εφαρμογές, εργαλεία ανάπτυξης, servers κλπ.
- Φυσικοί Πόροι: υλικό υπολογιστών, εξοπλισμός τηλεπικοινωνιών, αποθηκευτικά μέσα κλπ.
- Δικτυακός Εξοπλισμός: μηχανισμοί προστασίας (firewalls, anti-virus κλπ),

Αποδεκτή Χρήση των Πληροφοριακών Πόρων

Η εταιρεία ορίζει τους κανόνες για την αποδεκτή χρήση των πληροφοριών και των πληροφοριακών της συστημάτων, σύμφωνα με το βαθμό κρισιμότητάς τους. Σκοπός είναι η διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών και των συστημάτων και η αποτροπή επιβλαβών συμβάντων που μπορεί να προκύψουν από την κακή χρήση των παραπάνω. Όλοι οι χρήστες οφείλουν να είναι σε συμμόρφωση με τους κανόνες αυτούς και απαγορεύεται να προβαίνουν σε μη επιτρεπόμενες ενέργειες. Οι χρήστες οφείλουν να χρησιμοποιούν τους πόρους που τους παρέχονται με ασφαλή και νόμιμο τρόπο. Κάθε προσπάθεια μείωσης του επιπέδου ασφάλειας των πληροφοριακών συστημάτων απαγορεύεται αυστηρά. Απαγορεύεται κάθε είδους χρήση, εγκατάσταση και αντιγραφή παράνομου λογισμικού στα πληροφοριακά συστήματα της εταιρείας. Οι χρήστες δεν επιτρέπεται να εγκαθιστούν μη εξουσιοδοτημένο λογισμικό, καθώς υπάρχει σοβαρός κίνδυνος το λογισμικό αυτό να είναι μολυσμένο με ιούς

υπολογιστών, το οποίο δύναται να βλάψει τις πληροφορίες και τα συστήματα του Οργανισμού. Η χρήση των πληροφοριακών συστημάτων της εταιρείας παρέχεται στο προσωπικό της ως εργαλείο διεξαγωγής επιχειρηματικών δραστηριοτήτων.

Αποδεκτή Χρήση Συνθηματικών

Όλοι οι χρήστες, ιδιαίτερα με προνομιούχα δικαιώματα (π.χ. administrator), πρέπει να χρησιμοποιούν καλές πρακτικές αναφορικά με την επιλογή και τη χρήση των συνθηματικών που χρησιμοποιούν για να αποκτήσουν πρόσβαση στα πληροφοριακά συστήματα της εταιρείας. Κάθε χρήστης είναι υπεύθυνος για την ασφαλή χρήση του συνθηματικού του. Τα συνθηματικά πρέπει να έχουν τουλάχιστον τα ακόλουθα χαρακτηριστικά:

- Να αποτελούνται τουλάχιστον από 8 χαρακτήρες
- Να περιέχουν αλφαριθμητικά
- Να περιέχουν σύμβολα Τα συνθηματικά πρέπει να αλλάζουν ανά τακτά χρονικά διαστήματα, τουλάχιστον κάθε έξι μήνες.

Μη Αποδεκτή Χρήση Συνθηματικών Οι χρήστες δεν πρέπει να καταγράφουν και να φυλάσσουν τα συνθηματικά τους σε εμφανή σημεία. Σε κάθε περίπτωση, το συνθηματικό πρέπει να θεωρείται εμπιστευτική πληροφορία. Οι χρήστες δεν πρέπει να αποστέλλουν τα συνθηματικά μέσω του ηλεκτρονικού ταχυδρομείου. Οι χρήστες πρέπει να αποφεύγουν τη χρήση αυτόματης συμπλήρωσης (απομνημόνευσης) των συνθηματικών στους σταθμούς εργασίας ή/και στους φορητούς υπολογιστές.

Ασφαλής Χρήση Φορητών Υπολογιστών και Φορητών Αποθηκευτικών Μέσων

Η χρήση προσωπικών φορητών υπολογιστών και φορητών αποθηκευτικών μέσων δεν είναι επιτρεπτή. Οι χρήστες μπορούν να χρησιμοποιούν φορητούς υπολογιστές και μέσα που τους παρέχει ο Οργανισμός στο πλαίσιο της διεξαγωγής των εργασιακών τους καθηκόντων. Η παροχή φορητών υπολογιστών και μέσων αποσκοπεί στην εκπλήρωση των εργασιακών καθηκόντων των χρηστών.

Αποδεκτή Χρήση Ηλεκτρονικού Ταχυδρομείου και Διαδικτύου

Η χρήση του ηλεκτρονικού ταχυδρομείου και του διαδικτύου γίνεται στο πλαίσιο της διευκόλυνσης της διεξαγωγής των εργασιακών καθηκόντων των χρηστών. Πιο συγκεκριμένα:

- Επικοινωνία μεταξύ των υπαλλήλων της εταιρείας και των εξωτερικών συνεργατών στο πλαίσιο των εργασιακών αναγκών
- Μετάδοση των πληροφοριών, οι οποίες σχετίζονται με τις λειτουργίες της εταιρείας
- Ενημέρωση των χρηστών στο πλαίσιο των εργασιακών τους καθηκόντων Οι χρήστες πρέπει να είναι προσεκτικοί με τα ηλεκτρονικά μηνύματα από άγνωστους αποστολείς ή και με τη χρήση των επισυναπτόμενων αρχείων καθώς ενδέχεται να περιέχουν ιούς ή συνδέσεις σε παράνομες ιστοσελίδες.