ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

PUBLICSOFT IKE

Περιεχόμενα

Πεδίο

Αυτή η πολιτική ισχύει για τις οντότητες και το προσωπικό της **PUBLICSOFT IKE (εφεξής «η Εταιρεία»)**, για όλα τα περιληφθέντα πρόσωπα ή οντότητες και όλα τα περιληφθέντα συστήματα σε όλες τις εγκαταστάσεις που χρησιμοποιούν στην υποδομή τεχνολογίας πληροφοριών της.

Το πεδίο της πολιτικής ασφαλείας πληροφοριών περιλαμβάνει την προστασία της εμπιστευτικότητας, της ακεραιότητας, και της διαθεσιμότητας των πληροφοριών.

Αυτή η πολιτική ισχύει για όλα τα στοιχεία, το υλικό, τις πληροφορίες, και τις πληροφορίες προσδιορισμού ταυτότητας (PII) και άλλες κατηγορίες προστατευμένων πληροφοριών με οποιαδήποτε μορφή (φυσικό, ηλεκτρονικό, προφορικό κ.λπ.) που ανήκει ή ελέγχεται από την Εταιρεία.

Δήλωση Πολιτικής

Είναι η πολιτική εκείνων των πληροφοριών της Εταιρείας, όπως καθορίζεται προηγουμένως, σε όλες τις μορφές του γραπτές, προφορικές, καταγραμμένες ηλεκτρονικά ή τυπωμένες, που θα προστατευθούν από την τυχαία ή σκόπιμη αναρμόδια χρήση, την τροποποίηση, την καταστροφή ή την κοινοποίηση σε όλο τον κύκλο ζωής τους από αναρμόδιο ή εξουσιοδοτημένο προσωπικό χωρίς κατάλληλες και απαραίτητες άδειες. Αυτή η προστασία περιλαμβάνει ένα κατάλληλο επίπεδο ασφάλειας στα δεδομένα, τις πληροφορίες, τον εξοπλισμό, και το λογισμικό που χρησιμοποιείται για τη διαδικασία επεξεργασίας, αποθήκευσης και διαβίβασης των σωστών πληροφοριών.

Η Εταιρεία είναι αρμόδια για τις λειτουργούσες εγκαταστάσεις πληροφορικής (IT) που μεγιστοποιούν τη φυσική και ηλεκτρονική ασφάλεια, παρέχουν την αιτιολογημένη προστασία για τα συστήματα πληροφορικής (IT) από τις φυσικές ή άλλες καταστροφές, και ελαχιστοποιούν τους κινδύνους κυβερνοαπειλής για τα δεδομένα και τα συστήματα του.

Όλες οι οντότητες και το προσωπικό της Εταιρείας θα επεκτείνουν και θα χρησιμοποιήσουν τα συστήματα πληροφορικής (IT) και τις υπηρεσίες με τρόπους που θα μετριάζουν τους κινδύνους κυβερνοαπειλής, θα μεγιστοποιούν τη φυσική ασφάλεια των συστημάτων πληροφορικής, και θα ελαχιστοποιούν τους μη αποδεκτούς κινδύνους για τα συστήματα πληροφορικής και τα δεδομένα (data) από φυσικές καταστροφές (συλλογικά, «κίνδυνοι κυβερνοαπειλής»).

Ως μέσο μείωσης και μετριασμού κινδύνων κυβερνοαπειλών στην Εταιρεία όσον αφορά τις οντότητες και το προσωπικό, είναι το να χρησιμοποιούν τις ασφαλείς εγκαταστάσεις, την κοινή υποδομή τεχνολογίας πληροφοριών και τις υπηρεσίες που παρέχονται για χρήση από την Εταιρεία για την επίτευξη της καθημερινής εργασίας τους.

Στόχοι ασφαλείας πληροφοριών (Key Point Indicators)

Καταγράφουμε τους παρακάτω στόχους:

- Να παρέχονται διοικητικές κατευθύνσεις και υποστήριξη στην ασφάλεια πληροφοριών σύμφωνα με τις επιχειρησιακές απαιτήσεις και τους σχετικούς νόμους και τους κανονισμούς.
- Να θεσπίζεται το κατάλληλο διοικητικό πλαίσιο που θα δύναται να ελέγξει την εφαρμογή και τη λειτουργία της ασφαλείας πληροφοριών μέσα στον οργανισμό.
- Να εξασφαλίζεται ότι οι υπάλληλοι και οι ανάδοχοι καταλαβαίνουν τις ευθύνες τους, είναι κατάλληλοι για τους ρόλους για τους οποίους εξετάζονται, γνωρίζουν και εκπληρώνουν τις ευθύνες τους στην ασφαλείας πληροφοριών.
- Να προσδιορίζονται και να προστατεύονται τα περιουσιακά στοιχεία του οργανισμού με τον καθορισμό των κατάλληλων ευθυνών προστασίας.
- Να εξασφαλίζεται ότι οι πληροφορίες προστατεύονται ανάλογα με τη σημασία που έχουν για τον οργανισμό.
- Να εξασφαλίζονται σωστές και ασφαλείς διαδικασίες στις εγκαταστάσεις επεξεργασίας πληροφοριών.
- Να εξασφαλίζεται ότι οι πληροφορίες προστατεύονται στα δίκτυα επικοινωνιών και στις υποστηρικτές εγκαταστάσεις επεξεργασίας πληροφοριών.
- Να εξασφαλίζεται η προστασία των περιουσιακών στοιχείων του οργανισμού και των πληροφοριών που έχουν πρόσβαση οι προμηθευτές.
- Η συνέχεια στην ασφάλεια πληροφοριών θα πρέπει να είναι ενσωματωμένη στα συστήματα διαχείρισης της επιχειρησιακής συνέχειας του οργανισμού.
- Να εξασφαλίζεται η διαθεσιμότητα των εγκαταστάσεων επεξεργασίας πληροφοριών.
- Να αποφεύγονται οι παραβιάσεις των νομικών, θεσμικών, ρυθμιστικών, ή συμβατικών υποχρεώσεων που αφορούν την ασφάλεια πληροφοριών και οποιωνδήποτε απαιτήσεων ασφάλειας.
- Να εξασφαλίζεται ότι η ασφάλεια πληροφοριών εφαρμόζεται και λειτουργεί σύμφωνα με τις οργανωτικές πολιτικές και διαδικασίες του οργανισμού.

Υποχρέωση

Η ανώτατη διοίκηση της Εταιρείας είναι αρμόδια και δεσμευμένη σε σχέση με την ασφάλεια πληροφοριών για:

- να διατυπώσει και να αναθεωρήσει αυτήν την πολιτική ασφαλείας πληροφοριών,
- να εγκρίνει και να αναθεωρήσει όλες τις διαδικασίες, τη δράση και τις πολιτικές που προκύπτουν από αυτήν την πολιτική,

- να παρέχει όλους τους απαραίτητους πόρους για να ικανοποιήσει όλες τις απαιτήσεις της ασφαλείας πληροφοριών του οργανισμού,
- να βελτιώνει συνεχώς το σύστημα διαχείρισης ασφαλείας πληροφοριών και
- να πάρει τις κατάλληλες αποφάσεις σε σχέση με την ασφάλεια πληροφοριών

Ορισμοί ασφαλείας πληροφοριών

Διαθεσιμότητα: Εξασφάλιση της έγκαιρης και αξιόπιστης πρόσβασης και χρήσης των πληροφοριών.

Εμπιστευτικότητα: Διατήρηση των εξουσιοδοτημένων περιορισμών στην πρόσβαση πληροφοριών και την κοινοποίηση, συμπεριλαμβανομένων των μέσων για την προστασία της προσωπικής ιδιωτικότητας και των πληροφορίων που της ανήκουν.

Πληροφορία: Οποιαδήποτε επικοινωνία ή αντιπροσώπευση της γνώσης όπως γεγονότα, δεδομένα, ή απόψεις με οποιαδήποτε μέσο ή μορφή, συμπεριλαμβανομένου κειμένου, αριθμητικών, γραφικών, χαρτογραφικών, αφηγηματικών, ή οπτικοακουστικών μέσων.

Ασφάλεια πληροφοριών: Η προστασία των πληροφοριών και των συστημάτων πληροφοριών από την αναρμόδια πρόσβαση, χρήση, κοινοποίηση, διακοπή, τροποποίηση ή καταστροφή προκειμένου να παρέχεται ανεμπόδιστα η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα.

Σύστημα πληροφοριών: Ένα διακριτό σύνολο πηγών πληροφορίας που οργανώνεται για τη συλλογή, την επεξεργασία, τη συντήρηση, τη χρήση, τη διανομή, τη διάδοση, ή τη διάθεση των πληροφοριών.

Κίνδυνος ασφάλειας πληροφοριών (Cyber Risk): Ο κίνδυνος για τις οργανωτικές διαδικασίες (συμπεριλαμβανομένης της αποστολής, των λειτουργιών, της εικόνας και της φήμης του οργανισμού), τα οργανωτικά προτερήματα (υλικά ή άυλα), τα άτομα, άλλοι οργανισμοί καθώς και το Κράτος εξαιτίας της δυνητικής αναρμόδιας πρόσβασης, χρήσης, κοινοποίησης, διάσπασης, τροποποίησης ή της καταστροφής των πληροφοριών ή/και των συστημάτων πληροφοριών. (Βλέπε ***Κίνδυνος)***.

Ακεραιότητα: Η προστασία ενάντια στην αναρμόδια τροποποίηση ή την καταστροφή πληροφοριών που περιλαμβάνει και την εξασφάλιση της μη απάρνησης ευθύνης και της αυθεντικότητας των πληροφοριών.

Κίνδυνος: Ένα μέτρο του βαθμού στον οποίο μια οντότητα απειλείται από μια πιθανή περίσταση ή ένα γεγονός, και τυπικά μια λειτουργία κατά την οποία:

(i) οι δυσμενείς επιδράσεις που θα προκύπταν εάν η περίσταση ή το γεγονός εμφανιζόταν και

(ii) η πιθανότητα εμφάνισης.