Πολιτική Προσωπικών Συσκευών

Σκοπός

Οι κινητές συσκευές, όπως τα smartphones, οι υπολογιστές tablet και οι υπολογιστές laptop, αποτελούν σημαντικά εργαλεία για τον οργανισμό και η χρήση τους υποστηρίζεται για την επίτευξη επιχειρηματικών στόχων. Ωστόσο, οι κινητές συσκευές (προσωπικές ή του Ινστιτούτου) αντιπροσωπεύουν επίσης σημαντικό κίνδυνο για την ασφάλεια των πληροφοριών του Ινστιτούτου και την προστασία των δεδομένων. Εάν δεν εφαρμοστούν οι κατάλληλες πολιτικές και διαδικασίες ασφάλειας, οι κινητές συσκευές μπορούν να αποτελέσουν αγωγό για μη εξουσιοδοτημένη πρόσβαση στις πληροφορίες του οργανισμού και στην πληροφοριακή υποδομή. Αυτό μπορεί να οδηγήσει σε δαπανηρές διαρροές δεδομένων και σε μόλυνση των συστημάτων.

Η συγκεκριμένη πολιτική έχει ως στόχο την προστασία των πληροφοριακών περιουσιακών στοιχείων του Ινστιτούτο προκειμένου να διαφυλάξει τις πληροφορίες, τους πελάτες, τους ασθενείς/εξεταζόμενους την πνευματική ιδιοκτησία και τη φήμη του. Το παρόν έγγραφο περιγράφει ένα σύνολο πρακτικών και απαιτήσεων για την ασφαλή χρήση όλων των κινητών συσκευών κατά την πρόσβαση στο δίκτυο του Ινστιτούτου και αποσκοπεί στην προστασία της ασφάλειας και της ακεραιότητας των πληροφοριών και των πληροφοριακών υποδομών του Ινστιτούτου. Το Ινστιτούτο διατηρεί το δικαίωμα να περιορίσει τη χρήση κινητών συσκευών εάν οι χρήστες δεν συμμορφώνονται με τις πολιτικές και τις διαδικασίες που περιγράφονται παρακάτω.

Πεδίο Εφαρμογής

Η πολιτική αυτή αφορά όλες τις κινητές συσκευές (smartphones και υπολογιστές), είτε ανήκουν στο Ινστιτούτο είτε ανήκουν σε εργαζομένους, οι οποίες έχουν πρόσβαση σε δίκτυα του Ινστιτούτου, πληροφορίες και συστήματα, με εξαίρεση τους φορητούς υπολογιστές που διαχειρίζεται ο Υπεύθυνος Πληροφορικής. Περιορισμένες εξαιρέσεις από την πολιτική ενδέχεται να προκύψουν σε περιπτώσεις που υπάρχει ανάγκη. Ωστόσο, η αξιολόγηση κινδύνου πρέπει να διενεργείται από τον Υπεύθυνο Ασφάλειας Πληροφοριών και να χορηγείται εκ των προτέρων γραπτή έγκριση από τη Διοίκηση.

Αποδεκτή Χρήση

- Το Ινστιτούτο ορίζει ως αποδεκτή χρήση τις δραστηριότητες που άμεσα ή έμμεσα υποστηρίζουν τη λειτουργία του Ινστιτούτου.
- Απαγορεύεται η πρόσβαση σε παράνομους / απαγορευμένους ιστότοπους κατά τη διάρκεια των ωρών εργασίας ή ενώ οι εργαζόμενοι είναι συνδεδεμένοι με το δίκτυο του Ινστιτούτου. Τέτοιοι ιστότοποι περιλαμβάνουν, αλλά δεν περιορίζονται σε:
    - Ιστοσελίδες πορνογραφικού περιεχομένου,
    - Ιστοσελίδες παιδικής πορνογραφίας,
    - Ιστοσελίδες τυχερών παιγνίων, κ.λπ.
- Τα δεδομένα θέσης είναι απενεργοποιημένα, εκτός εάν τα έχει ενεργοποιήσει ο ίδιος ο εργαζόμενος.

- Οι κινητές συσκευές δεν επιτρέπεται να χρησιμοποιούνται για:
    - Αποθήκευση ή μετάδοση παράνομου υλικού
    - Αποθήκευση ή μετάδοση ιδιόκτητων πληροφοριών που ανήκουν σε άλλον οργανισμό
    - Παρενόχληση τρίτων ατόμων
    - Συμμετοχή σε δραστηριότητες έξω από το Ινστιτούτο
- Απαγορεύεται η εγκατάσταση εφαρμογών που δεν προέρχονται από το iTunes ή το Google Play.

Ασφάλεια Πληροφοριών

- Προκειμένου να αποφευχθεί η μη εξουσιοδοτημένη πρόσβαση, οι κινητές συσκευές πρέπει να προστατεύονται με κωδικό πρόσβασης, χρησιμοποιώντας τα χαρακτηριστικά της συσκευής.
- Ο κωδικός πρόσβασης είναι αυστηρά προσωπικός και δεν πρέπει να τον γνωρίζει κανείς άλλος από το επαγγελματικό, οικογενειακό ή φιλικό περιβάλλον του κατόχου της συσκευής.
- Οι κωδικοί πρόσβασης πρέπει να περιέχουν έναν ελάχιστο αριθμό χαρακτήρων και να αλλάζουν σύμφωνα με την Πολιτική Κωδικών Πρόσβασης. Ο κωδικός πρόσβασης δεν πρέπει να είναι ο ίδιος με τα υπόλοιπα διαπιστευτήρια που χρησιμοποιούνται στο πλαίσιο του οργανισμού. Οι εργαζόμενοι είναι υπεύθυνοι για την τακτική αλλαγή των κωδικών πρόσβασης στις κινητές συσκευές τους. Συνίσταται η αλλαγή του κωδικού τουλάχιστον κάθε 2 μήνες και οπωσδήποτε στην περίπτωση που υπάρχει υπόνοια διαρροής του σε άλλο πρόσωπο.

Προστασία προσωπικών δεδομένων (συμμόρφωση με GDPR & ISO 27701)

Σε συμμόρφωση με τον GDPR και το ISO 27701, δεν πρέπει να αποθηκεύονται προσωπικά δεδομένα που χειρίζεται το ΙΝΕΒ στο πλαίσιο της λειτουργίας και των ερευνητικών δραστηριοτήτων σε προσωπικές συσκευές. Εάν είναι απαραίτητη η επεξεργασία ή αποθήκευση προσωπικών δεδομένων σε προσωπική συσκευή, πρέπει να ληφθεί ρητή γραπτή άδεια από το Ινστιτούτο. Επιπλέον, πρέπει να τεκμηριώνεται η περίοδος διατήρησης των δεδομένων και να εφαρμόζονται κατάλληλα τεχνικά και οργανωτικά μέτρα (όπως κρυπτογράφηση, έλεγχος πρόσβασης και μηχανισμοί ασφαλούς διαγραφής) για να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των προσωπικών δεδομένων. Όλοι οι χρήστες πρέπει να συμμορφώνονται με τις πολιτικές προστασίας προσωπικών δεδομένων για τον μετριασμό των κινδύνων που συνδέονται με μη εξουσιοδοτημένη πρόσβαση, διαρροή δεδομένων ή μη συμμόρφωση με τις κανονιστικές απαιτήσεις.

Κίνδυνοι/ Υποχρεώσεις / Αποποίηση Ευθυνών

- Οι χαμένες ή κλεμμένες κινητές συσκευές πρέπει να αναφέρονται στον Υπεύθυνο Ασφάλειας Πληροφοριών. Οι υπάλληλοι είναι υπεύθυνοι για την κοινοποίηση στον πάροχο της κινητής τηλεφωνίας της απώλειας μιας προσωπικής κινητής συσκευής.

- Εάν ένας εργαζόμενος υποψιάζεται ότι έχει γίνει μη εξουσιοδοτημένη πρόσβαση στα δεδομένα του Ινστιτούτου μέσω μιας κινητής συσκευής, πρέπει να αναφέρει το περιστατικό αμέσως στον Υπεύθυνο Ασφάλειας Πληροφοριών.
- Ο εργαζόμενος αναμένεται να χρησιμοποιεί τις κινητές συσκευές του με ηθικό τρόπο ανά πάσα στιγμή και να συμμορφώνεται με την πολιτική αποδεκτής χρήσης του Ινστιτούτου όπως περιγράφεται παραπάνω.

Δήλωση Αποδοχής της Πολιτικής Προσωπικών Συσκευών

Έχω διαβάσει και κατανοήσει την Πολιτική Προσωπικών Συσκευών και συμφωνώ να συμμορφωθώ με τις πολιτικές και διαδικασίες που ορίζονται σε αυτή. Κατανοώ ότι η διατήρηση αντιγράφων ασφαλείας των πληροφοριών που είναι αποθηκευμένες στην συσκευή είναι δική μου ευθύνη.

Ονοματεπώνυμο εργαζομένου

Υπογραφή

Ημερομηνία