

ΠΟΛΙΤΙΚΗ ΚΑΘΑΡΟΥ ΓΡΑΦΕΙΟΥ (CLEAN DESK POLICY)

1. ΕΙΣΑΓΩΓΗ

Η Πολιτική Καθαρού Γραφείου (Clean Desk Policy) του «BENIZEΛΕΙΟΥ ΝΟΣΟΚΟΜΕΙΟΥ» έχει ως κύριο στόχο να ενισχύσει την ασφάλεια, την προστασία και την εμπιστευτικότητα των ευαίσθητων δεδομένων / πληροφοριών σε όλους τους υπολογιστές και εκτυπωτές του δικτύου περιορίζοντας με αυτόν τον τρόπο την έκθεση / διαρροή τους στο χώρο εργασίας.

Τα ευαίσθητα / εμπιστευτικά δεδομένα μπορούν να βρίσκονται είτε σε έγγραφα έντυπης μορφής, είτε σε συσκευές αποθήκευσης (π.χ. σκληροί δίσκοι, usb) είτε σε συσκευές υλικού (hardware). Για το λόγο αυτό, όλα τα παραπάνω θα πρέπει να “ασφαλιζονται” κατάλληλα όταν ο σταθμός εργασίας βρίσκεται σε αδράνεια ή όταν ο υπάλληλος απομακρύνεται από αυτόν.

Κύριος στόχος της πολιτικής καθαρού γραφείου είναι να μειωθεί ο κίνδυνος της μη εξουσιοδοτημένης πρόσβασης στους υπολογιστές του νοσοκομείου ή ακόμα και η απώλεια / καταστροφή σημαντικών πληροφοριών.

Η Πολιτική Καθαρού Γραφείου (Clean Desk Policy) είναι ένα σημαντικό ζήτημα που αφορά την προστασία της ασφάλειας καθώς και της ιδιωτικότητας του νοσοκομείου και περιλαμβάνεται στους κανονισμούς του ISO 27001/17799 και του ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (GDPR E.E. 679/2016)

2. ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η Πολιτική Καθαρού Γραφείου (Clean Desk Policy) αφορά όλο το μόνιμο προσωπικό καθώς και όλους όσους εργάζονται στο νοσοκομείο με οποιαδήποτε μορφή σύμβασης.

3. ΠΟΛΙΤΙΚΗ

Οι γενικοί κανόνες της πολιτικής καθαρού γραφείου είναι :

- Οι εργαζόμενοι διασφαλίζουν ότι όλες οι ευαίσθητες / εμπιστευτικές πληροφορίες σε έντυπη μορφή, παραμένουν ασφαλείς σε κλειδωμένο συρτάρι στο τέλος της εργάσιμης ημέρας αλλά και όταν αναμένεται να

απουσιάζουν για μεγάλο χρονικό διάστημα (άδεια). Το ίδιο ισχύει για τις πληροφορίες σε ηλεκτρονική μορφή.

- Οι σταθμοί εργασίας (υπολογιστές, φορητοί, tablets) θα πρέπει να κλειδώνονται (αποσυνδεδεμένοι ή απενεργοποιημένοι) για όσο ο χώρος εργασίας είναι κενός χωρίς επιτήρηση και στο τέλος της ημέρας.
- Οι συσκευές μαζικής αποθήκευσης, όπως δίσκοι CD, DVD ή USB, πρέπει να αντιμετωπίζονται ως ευαίσθητες και κατά συνέπεια, πρέπει να παραμένουν ασφαλείς σε κλειδωμένο συρτάρι.
- Φορητοί υπολογιστές και tablets πρέπει να κλειδώνονται σε κάποιο συρτάρι / ντουλάπα όταν δε χρησιμοποιούνται.
- Κλειδιά που χρησιμοποιούνται για την πρόσβαση σε συρτάρια ή οτιδήποτε περιέχει ευαίσθητες / εμπιστευτικές πληροφορίες, δε θα πρέπει να παραμένουν σε κοινή θέα και χωρίς επιτήρηση.
- Απόρρητα και εμπιστευτικά έγγραφα που δεν είναι πλέον χρήσιμα για τον υπάλληλο πρέπει να καταστρέφονται σε καταστροφείς εγγράφων.
- Οποιοδήποτε ευαίσθητο και εμπιστευτικό έγγραφο εκτυπωθεί θα πρέπει να αφαιρείται αμέσως από τον εκτυπωτή ή τις συσκευές fax.
- Η εκτύπωση φυσικών αντιγράφων θα πρέπει να προορίζεται για στιγμές απόλυτης ανάγκης. Τα έγγραφα πρέπει να προβάλλονται, να μοιράζονται και να διαχειρίζονται ηλεκτρονικά όποτε είναι δυνατόν.
- Οι κωδικοί πρόσβασης, είναι προσωπικοί και δε θα πρέπει να δίνονται σε άλλους. Προσοχή θα πρέπει να δίδεται στην αναγραφή τους σε σημεία τα οποία είναι προσβάσιμα και από άλλους πέραν του χρήστη.

4. ΣΥΜΜΟΡΦΩΣΗ

Η συμμόρφωση με την πολιτική θα επαληθεύεται μέσω διαφόρων μεθόδων, συμπεριλαμβανομένων, της περιοδικής παρακολούθησης και διενέργειας ελέγχων. Δεν υφίστανται εξαιρέσεις αναφορικά με μη συμμόρφωση με την πολιτική.

Εάν παρατηρήσετε ότι κάποια από τις συσκευές ή τα έγγραφά σας, λείπουν από τον χώρο σας ή εάν πιστεύετε ότι ο χώρος εργασίας σας έχει παραβιαστεί με οποιονδήποτε τρόπο, ενημερώστε αμέσως.