



ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΠΑΙΔΩΝ ΠΑΤΡΩΝ "ΚΑΡΑΜΑΝΔΑΝΕΙΟ"

ΑΥΤΟΤΕΛΕΣ ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΚΑΝΟΝΙΣΜΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗΣ ΠΡΟΣΒΑΣΗΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ



ΕΚΔΟΣΗ 1.0

ΠΑΤΡΑ 2026



Περιεχόμενα

1. Εισαγωγή.....	1
2. Πληροφοριακές Υποδομές και Συστήματα – Ορισμοί.....	2
3. Διαχειριστές Πληροφοριακών Συστημάτων	2
4. Ρόλοι και Αρμοδιότητες Νοσοκομείου	3
5. Κανόνες Χρηστών	4
6. Οδηγίες και Κατευθυντήριες Γραμμές Χρήσης Πληροφοριακών Συστημάτων	5
7. Διαχείριση Κωδικών Πρόσβασης.....	7
8. Χρήση Ηλεκτρονικού Ταχυδρομείου	7
9. Χρήση Διαδικτύου.....	8
10. Χρήση Προσωπικών Συσκευών	9
11. Τροποποιήσεις και Αλλαγές Πληροφοριακών Συστημάτων	9
12. Πολιτική Κυβερνοασφάλειας.....	10
13. Διαχείριση Περιστατικών Ασφάλειας Πληροφοριών.....	10
14. Διαχείριση Κακόβουλου Λογισμικού	11
15. Διαχείριση Επιθέσεων Ηλεκτρονικού Ψαρέματος (Phishing).....	11
16. Αντίγραφα Ασφαλείας και Ανάκτηση Δεδομένων	12
17. Σχέδιο Ανάκαμψης από Καταστροφή (Disaster Recovery).....	12
18. Κυρώσεις.....	13
19. Αναθεώρηση Κανονισμού	13
20. Αλγόριθμος Λειτουργίας και Χρήσης Πληροφοριακών Συστημάτων	14

1. Εισαγωγή

Το Γενικό Νοσοκομείο Παίδων Πατρών «Καραμανδάνειο» εφαρμόζει Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων, μέσω της οποίας διαμορφώνεται το πλαίσιο για την ασφαλή λειτουργία, διαχείριση και αξιοποίηση των πληροφοριακών υποδομών και συστημάτων του Νοσοκομείου.

Στο πλαίσιο της πολιτικής προσδιορίζονται:

- οι υποχρεώσεις και τα δικαιώματα των χρηστών των πληροφοριακών συστημάτων,
- οι όροι και οι κανόνες ορθής χρήσης του υπολογιστικού εξοπλισμού και των σχετικών υποδομών,
- οι διαδικασίες που αφορούν την πρόσβαση, επεξεργασία και διαχείριση των δεδομένων,
- τα απαιτούμενα οργανωτικά και τεχνικά μέτρα για την προστασία των πληροφοριακών συστημάτων.

Βασικός σκοπός του παρόντος κανονισμού είναι η ασφαλής, ορθή και απρόσκοπτη λειτουργία των πληροφοριακών συστημάτων του Νοσοκομείου, καθώς και η διασφάλιση των δεδομένων που αποθηκεύονται, επεξεργάζονται ή διακινούνται μέσω αυτών.

Ιδιαίτερη βαρύτητα αποδίδεται στην προστασία των δεδομένων προσωπικού χαρακτήρα και ιδίως των δεδομένων υγείας των ασθενών. Για τον σκοπό αυτό λαμβάνονται μέτρα για την πρόληψη περιστατικών που ενδέχεται να προκαλέσουν:

- απώλεια δεδομένων, είτε από αμέλεια είτε από τεχνικό ή άλλο συμβάν,
- μη επιτρεπτή ή κακόβουλη αξιοποίηση πληροφοριών,
- πρόσβαση σε πληροφοριακά συστήματα από μη εξουσιοδοτημένα πρόσωπα,
- αλλοίωση, καταστροφή ή μη εξουσιοδοτημένη μεταβολή δεδομένων,
- παράνομη ή μη επιτρεπόμενη γνωστοποίηση και διάδοση πληροφοριών.

Τα μέτρα και οι κανόνες που προβλέπονται στον παρόντα κανονισμό αποβλέπουν στη συνολική προστασία των πληροφοριακών υποδομών και στη διασφάλιση ότι η χρήση τους πραγματοποιείται σύμφωνα με την ισχύουσα νομοθεσία, τις αρχές δεοντολογίας και τις θεμελιώδεις απαιτήσεις ασφάλειας πληροφοριών.



2. Πληροφοριακές Υποδομές και Συστήματα – Ορισμοί

Ως Πληροφοριακές Υποδομές και Συστήματα του Νοσοκομείου νοείται το σύνολο του υλικού εξοπλισμού, των δικτυακών υποδομών, των εφαρμογών και των λοιπών τεχνολογικών μέσων που χρησιμοποιούνται για την καταχώριση, επεξεργασία, αποθήκευση, διαχείριση και διακίνηση δεδομένων.

Στις πληροφοριακές υποδομές περιλαμβάνονται ενδεικτικά:

- οι σταθμοί εργασίας και οι ηλεκτρονικοί υπολογιστές,
- οι εξυπηρετητές (servers),
- οι εκτυπωτές και οι λοιπές περιφερειακές συσκευές,
- τα συστήματα και τα μέσα αποθήκευσης δεδομένων,
- ο ενεργός δικτυακός εξοπλισμός, όπως switches και routers,
- οι καλωδιώσεις, τα τοπικά δίκτυα (LAN) και οι υποδομές ασύρματης δικτύωσης,
- οι εφαρμογές και τα συστήματα λογισμικού,
- οι βάσεις δεδομένων,
- οι υπηρεσίες ηλεκτρονικού ταχυδρομείου,
- οι υπηρεσίες πρόσβασης και χρήσης του διαδικτύου.

Το σύνολο των ανωτέρω αποτελεί περιουσιακό στοιχείο του Νοσοκομείου και χρησιμοποιείται για την κάλυψη των υπηρεσιακών αναγκών και την υποστήριξη της λειτουργίας των διοικητικών, ιατρικών και λοιπών υπηρεσιών του.

3. Διαχειριστές Πληροφοριακών Συστημάτων

Ως Διαχειριστές των Πληροφοριακών Συστημάτων του Νοσοκομείου ορίζονται:

- το Αυτοτελές Τμήμα Οργάνωσης και Πληροφορικής του Νοσοκομείου,
- οι χρήστες στους οποίους έχει χορηγηθεί σχετική εξουσιοδότηση και οι οποίοι έχουν οριστεί από το αρμόδιο Αυτοτελές Τμήμα Οργάνωσης και Πληροφορικής για την εκτέλεση συγκεκριμένων διαχειριστικών αρμοδιοτήτων.
- εξωτερικοί συνεργάτες ή εταιρείες τεχνικής υποστήριξης, εφόσον διαθέτουν ενεργές συμβάσεις συντήρησης και υποστήριξης των πληροφοριακών συστημάτων.

Οι Διαχειριστές Πληροφοριακών Συστημάτων έχουν την ευθύνη για:

- την ομαλή λειτουργία και τη συντήρηση των πληροφοριακών υποδομών,
- την εύρυθμη λειτουργία των εφαρμογών και των πληροφοριακών συστημάτων,



- την εφαρμογή των προβλεπόμενων πολιτικών και μέτρων ασφάλειας,
- τη συνεχή παρακολούθηση της λειτουργίας του δικτύου και των υπολογιστικών συστημάτων,
- την αντιμετώπιση τεχνικών προβλημάτων και δυσλειτουργιών,
- την πραγματοποίηση περιοδικών ελέγχων στα πληροφοριακά συστήματα και στις υποδομές δικτύου,
- τη λήψη των απαραίτητων μέτρων για την αποτροπή μη εξουσιοδοτημένης πρόσβασης.

Στο πλαίσιο των αρμοδιοτήτων τους, οι Διαχειριστές έχουν τη δυνατότητα να προβαίνουν στις απαραίτητες τεχνικές ενέργειες για την αποκατάσταση της ομαλής και ασφαλούς λειτουργίας των συστημάτων, όπως:

- τερματισμό εφαρμογών,
- αποσύνδεση χρηστών από το δίκτυο,
- προσωρινή τροποποίηση ή απενεργοποίηση κωδικών πρόσβασης,
- αποσύνδεση συσκευών από το δίκτυο.

Το Νοσοκομείο διατηρεί το δικαίωμα να περιορίζει ή να ανακαλεί την πρόσβαση χρηστών στα πληροφοριακά συστήματα, όταν αυτό κρίνεται απαραίτητο για την προστασία και την ασφάλεια των συστημάτων και των δεδομένων.

4. Ρόλοι και Αρμοδιότητες Νοσοκομείου

Το Νοσοκομείο οφείλει να λαμβάνει όλα τα αναγκαία οργανωτικά και τεχνικά μέτρα, προκειμένου να διασφαλίζεται η ορθή εφαρμογή της Πολιτικής Ασφάλειας Πληροφοριακών Συστημάτων.

Στο πλαίσιο αυτό, το Νοσοκομείο:

- μεριμνά για την ασφάλεια των πληροφοριακών συστημάτων και των δεδομένων,
- διασφαλίζει την ακεραιότητα και την προστασία του πληροφοριακού και υπολογιστικού εξοπλισμού,
- εποπτεύει την ορθή και επιτρεπόμενη χρήση των πληροφοριακών υποδομών,
- πραγματοποιεί περιοδικούς ελέγχους στα πληροφοριακά συστήματα και στις δικτυακές υποδομές,
- λαμβάνει τα κατάλληλα μέτρα για την πρόληψη και αποτροπή μη εξουσιοδοτημένης πρόσβασης.



Οι πληροφοριακές εγκαταστάσεις και υποδομές του Νοσοκομείου προορίζονται αποκλειστικά για την κάλυψη των υπηρεσιακών και λειτουργικών αναγκών του. Δεν επιτρέπεται η αξιοποίησή τους για εμπορικούς σκοπούς, προσωπική χρήση ή για οποιαδήποτε άλλη δραστηριότητα που δεν συνδέεται άμεσα με την αποστολή και τη λειτουργία του Νοσοκομείου.

5. Κανόνες Χρηστών

Τα πληροφοριακά συστήματα του Νοσοκομείου διαχειρίζονται δεδομένα στα οποία περιλαμβάνονται ευαίσθητες πληροφορίες και δεδομένα που αφορούν την υγεία των ασθενών.

Η επεξεργασία των δεδομένων αυτών πραγματοποιείται σύμφωνα με:

- τον Ευρωπαϊκό Κανονισμό για την Προστασία Δεδομένων (ΕΕ 2016/679 – GDPR),
- τον Νόμο 4624/2019,
- τις εσωτερικές πολιτικές και διαδικασίες ασφάλειας του Νοσοκομείου.

Οι χρήστες των πληροφοριακών συστημάτων έχουν υποχρέωση να προστατεύουν το απόρρητο των πληροφοριών που συλλέγουν, χρησιμοποιούν ή επεξεργάζονται και να εξασφαλίζουν, στο πλαίσιο των αρμοδιοτήτων τους, την ακεραιότητα και την ασφαλή διαχείριση των δεδομένων

Ειδικότερα, οι χρήστες οφείλουν:

- να χρησιμοποιούν τα πληροφοριακά συστήματα **αποκλειστικά για την εκτέλεση των υπηρεσιακών τους καθηκόντων**,
- να συμμορφώνονται με την **Πολιτική Ασφάλειας του Νοσοκομείου**,
- να διασφαλίζουν την προστασία των δεδομένων που διαχειρίζονται,
- να αποφεύγουν οποιαδήποτε ενέργεια μπορεί να επηρεάσει αρνητικά ή να θέσει σε κίνδυνο την ασφαλή και ομαλή λειτουργία των πληροφοριακών συστημάτων.



Δικαίωμα πρόσβασης στα πληροφοριακά συστήματα παρέχεται αποκλειστικά σε εργαζομένους του Νοσοκομείου. Η πρόσβαση τρίτων προσώπων επιτρέπεται μόνο κατόπιν προηγούμενης έγκρισης της Διοίκησης.

Για την ενεργοποίηση της πρόσβασης στα πληροφοριακά συστήματα απαιτείται η υποβολή σχετικού αιτήματος προς το Αυτοτελές Τμήμα Οργάνωσης και ς Πληροφορικής. Ενδεικτικά, τα αιτήματα μπορεί να αφορούν:

- χορήγηση κωδικού πρόσβασης,
- δημιουργία υπηρεσιακού λογαριασμού ηλεκτρονικού ταχυδρομείου,
- παροχή δυνατότητας απομακρυσμένης πρόσβασης μέσω VPN.

Διαδικασία έγκρισης

Κάθε νέος χρήστης οφείλει να υποβάλλει το προβλεπόμενο αίτημα προς το Αυτοτελές Τμήμα Οργάνωσης και ς Πληροφορικής. Το αίτημα συνυπογράφεται από τον αρμόδιο προϊστάμενο ή διευθυντή της υπηρεσίας στην οποία ανήκει ο χρήστης και αναφέρει με σαφήνεια τα δικαιώματα πρόσβασης που απαιτούνται για την άσκηση των καθηκόντων του.

Οποιαδήποτε υπηρεσιακή μεταβολή επηρεάζει τα υφιστάμενα δικαιώματα πρόσβασης πρέπει να γνωστοποιείται **άμεσα** στο Αυτοτελές Τμήμα Οργάνωσης και Πληροφορικής, προκειμένου να πραγματοποιείται η αντίστοιχη τροποποίηση, ανάκληση ή επικαιροποίηση των σχετικών δικαιωμάτων.

Οι προσωπικοί κωδικοί πρόσβασης είναι αυστηρά εμπιστευτικοί και απαγορεύεται η κοινοποίησή τους σε οποιοδήποτε άλλο πρόσωπο.

Σε κάθε χρήστη αποδίδονται συγκεκριμένα και διαβαθμισμένα δικαιώματα πρόσβασης, ανάλογα με τη θέση, τις αρμοδιότητες και το αντικείμενο εργασίας του.

Κάθε χρήστης φέρει την ευθύνη για τις ενέργειες που πραγματοποιούνται μέσω του προσωπικού του λογαριασμού.

6. Οδηγίες και Κατευθυντήριες Γραμμές Χρήσης Πληροφοριακών Συστημάτων

Η ασφαλής και ορθή χρήση των πληροφοριακών συστημάτων αποτελεί ευθύνη όλων των χρηστών. Οι εργαζόμενοι που διαθέτουν πρόσβαση στις πληροφοριακές υποδομές του Νοσοκομείου οφείλουν να ακολουθούν τις καθορισμένες οδηγίες και τις πολιτικές



ασφάλειας, ώστε να προστατεύονται οι πληροφορίες και να διασφαλίζεται η εύρυθμη λειτουργία των συστημάτων.

Οι χρήστες οφείλουν:

- να προστατεύουν τα δεδομένα που διαχειρίζονται και να αποτρέπουν την πρόσβαση σε αυτά από μη εξουσιοδοτημένα πρόσωπα,
- να μην αποθηκεύουν ευαίσθητα δεδομένα σε μέσα αποθήκευσης που δεν έχουν εγκριθεί για τον συγκεκριμένο σκοπό,
- να κλειδώνουν τον υπολογιστή τους κάθε φορά που απομακρύνονται από τον χώρο εργασίας τους,
- να μην αφήνουν ενεργές συνεδρίες εφαρμογών που περιέχουν ή διαχειρίζονται ευαίσθητα δεδομένα,
- να διασφαλίζουν ότι τα έγγραφα που εκτυπώνονται δεν παραμένουν εκτεθειμένα ή χωρίς επίβλεψη σε κοινόχρηστους εκτυπωτές.

Επιπλέον, δεν επιτρέπεται:

- η εγκατάσταση οποιουδήποτε λογισμικού χωρίς προηγούμενη έγκριση του Αυτοτελούς Τμήματος Οργάνωσης και Πληροφορικής.
- η μη εξουσιοδοτημένη μεταβολή των ρυθμίσεων του λειτουργικού συστήματος ή του δικτύου,
- η χρήση εφαρμογών ή προγραμμάτων που ενδέχεται να επηρεάσουν την ασφάλεια, τη διαθεσιμότητα ή την απόδοση των πληροφοριακών συστημάτων.
- η χρήση εξωτερικών μέσων αποθήκευσης, όπως USB, εξωτερικοί σκληροί δίσκοι και συναφή μέσα, χωρίς προηγούμενη έγκριση.

Απαγορεύεται αυστηρά η εγκατάσταση ή χρήση λογισμικού για το οποίο δεν υφίσταται νόμιμη άδεια χρήσης.

Οι χρήστες οφείλουν επίσης να ενημερώνουν άμεσα το Τμήμα Πληροφορικής όταν:

- διαπιστώνουν ασυνήθιστη ή μη αναμενόμενη συμπεριφορά κάποιου συστήματος,
- εμφανίζονται μηνύματα σφάλματος που ενδέχεται να υποδηλώνουν πρόβλημα ασφάλειας,



- υποψιάζονται ότι έχει παραβιαστεί ή χρησιμοποιηθεί από μη εξουσιοδοτημένο πρόσωπο ο λογαριασμός τους.

7. Διαχείριση Κωδικών Πρόσβασης

Οι κωδικοί πρόσβασης αποτελούν βασικό μηχανισμό για τον έλεγχο της πρόσβασης και την προστασία των πληροφοριακών συστημάτων.

Οι χρήστες υποχρεούνται:

- να διατηρούν τους προσωπικούς τους κωδικούς απολύτως εμπιστευτικούς,
- να μην καταγράφουν τους κωδικούς σε εμφανή ή εύκολα προσβάσιμα σημεία, όπως σημειώματα πάνω ή κοντά στον υπολογιστή,
- να μην κοινοποιούν ή γνωστοποιούν τους κωδικούς τους σε συναδέλφους ή άλλα πρόσωπα,
- να αλλάζουν τους κωδικούς πρόσβασης ανά τακτά χρονικά διαστήματα.

Οι κωδικοί πρόσβασης πρέπει:

- να διαθέτουν επαρκές μήκος,
- να αποτελούνται, όπου αυτό υποστηρίζεται, από συνδυασμό γραμμάτων, αριθμών και ειδικών χαρακτήρων,
- να μην βασίζονται σε απλές ή εύκολα προβλέψιμες προσωπικές πληροφορίες, όπως ημερομηνία γέννησης ή όνομα.

Εφόσον υπάρχει υποψία ότι ένας κωδικός πρόσβασης έχει γνωστοποιηθεί, υποκλαπεί ή εκτεθεί σε τρίτο πρόσωπο, ο χρήστης οφείλει να τον αλλάξει άμεσα και να ενημερώσει σχετικά το Αυτοτελές Τμήμα Οργάνωσης και Πληροφορικής.

8. Χρήση Ηλεκτρονικού Ταχυδρομείου

Η υπηρεσία ηλεκτρονικού ταχυδρομείου του Νοσοκομείου αποτελεί εργαλείο υπηρεσιακής επικοινωνίας και χρησιμοποιείται αποκλειστικά για την υποστήριξη των λειτουργικών και υπηρεσιακών αναγκών του οργανισμού.

Οι χρήστες οφείλουν να χρησιμοποιούν το υπηρεσιακό ηλεκτρονικό ταχυδρομείο με υπευθυνότητα και επαγγελματισμό.

**Δεν επιτρέπεται:**

- η χρήση υπηρεσιακών λογαριασμών ηλεκτρονικού ταχυδρομείου για προσωπικές δραστηριότητες που δεν συνδέονται με την εργασία,
- η αποστολή περιεχομένου προσβλητικού, παράνομου ή ακατάλληλου,
- η μαζική αποστολή μηνυμάτων χωρίς υπηρεσιακό λόγο,
- η γνωστοποίηση ή διαβίβαση εμπιστευτικών πληροφοριών χωρίς να έχουν ληφθεί τα κατάλληλα μέτρα προστασίας.

Οι χρήστες πρέπει να είναι ιδιαίτερα προσεκτικοί κατά τη λήψη και διαχείριση μηνυμάτων ηλεκτρονικού ταχυδρομείου που:

- προέρχονται από άγνωστους ή μη αναμενόμενους αποστολείς,
- περιλαμβάνουν ύποπτους συνδέσμους,
- συνοδεύονται από αρχεία άγνωστης ή αμφίβολης προέλευσης,
- ζητούν την καταχώριση ή γνωστοποίηση κωδικών πρόσβασης, προσωπικών στοιχείων ή άλλων εμπιστευτικών πληροφοριών.

Μηνύματα αυτού του τύπου ενδέχεται να αποτελούν απόπειρες ηλεκτρονικής εξαπάτησης (phishing) και πρέπει να αναφέρονται άμεσα στο Αυτοτελές Τμήμα Οργάνωσης και Πληροφορικής.

9. Χρήση Διαδικτύου

Η πρόσβαση στο διαδίκτυο παρέχεται στους εργαζομένους του Νοσοκομείου με σκοπό την υποστήριξη των υπηρεσιακών τους καθηκόντων, καθώς και την αναζήτηση επιστημονικών, διοικητικών ή άλλων πληροφοριών που σχετίζονται με το αντικείμενο της εργασίας τους.

Η χρήση του διαδικτύου πρέπει να πραγματοποιείται με υπευθυνότητα και σύμφωνα με τις ισχύουσες πολιτικές και απαιτήσεις ασφάλειας του οργανισμού.

Δεν επιτρέπεται:

- η πρόσβαση σε ιστοσελίδες που συνδέονται με παράνομες ή μη επιτρεπόμενες δραστηριότητες,
- η λήψη, διακίνηση ή χρήση παράνομου υλικού,
- η χρήση εφαρμογών διαμοιρασμού αρχείων (peer-to-peer),
- η εγκατάσταση επεκτάσεων, πρόσθετων ή λογισμικού μέσω διαδικτύου χωρίς προηγούμενη έγκριση.



Οι χρήστες οφείλουν να αποφεύγουν τη λήψη αρχείων από μη αξιόπιστες ή άγνωστες πηγές και να χρησιμοποιούν το διαδίκτυο με τρόπο που δεν θέτει σε κίνδυνο την ασφάλεια, την ακεραιότητα και την ομαλή λειτουργία των πληροφοριακών συστημάτων.

10. Χρήση Προσωπικών Συσκευών

Η σύνδεση προσωπικών συσκευών στο δίκτυο του Νοσοκομείου επιτρέπεται μόνο υπό συγκεκριμένες προϋποθέσεις και σύμφωνα με τους ισχύοντες κανόνες ασφάλειας.

Προσωπικές συσκευές, όπως κινητά τηλέφωνα, tablets και φορητοί υπολογιστές, μπορούν να συνδέονται αποκλειστικά στο δίκτυο επισκεπτών (guest network).

Δεν επιτρέπεται:

- η σύνδεση προσωπικών συσκευών στο εσωτερικό δίκτυο του Νοσοκομείου,
- η αποθήκευση δεδομένων υγείας ή άλλων υπηρεσιακών δεδομένων σε προσωπικές συσκευές,
- η μεταφορά ή αποθήκευση δεδομένων του Νοσοκομείου σε μέσα ή υπηρεσίες που δεν έχουν εγκριθεί από τον οργανισμό.

11. Τροποποιήσεις και Αλλαγές Πληροφοριακών Συστημάτων

Κάθε μεταβολή που αφορά τις πληροφοριακές υποδομές και τα συστήματα του Νοσοκομείου πρέπει να πραγματοποιείται αποκλειστικά από το Αυτοτελές Τμήμα Οργάνωσης και Πληροφορικής ή από συνεργάτες που διαθέτουν σχετική εξουσιοδότηση.

Οι αλλαγές αυτές μπορεί να περιλαμβάνουν:

- εγκατάσταση ή αντικατάσταση νέου εξοπλισμού,
- εγκατάσταση, αναβάθμιση ή τροποποίηση λογισμικού,
- αναβαθμίσεις πληροφοριακών συστημάτων,
- μεταβολές στις ρυθμίσεις ή στη διαμόρφωση του δικτύου,
- αλλαγές ή παρεμβάσεις στη δομή και λειτουργία των πληροφοριακών εφαρμογών.

Απαγορεύεται η αυθαίρετη ή μη εξουσιοδοτημένη παρέμβαση σε πληροφοριακά συστήματα από χρήστες που δεν διαθέτουν τα αντίστοιχα δικαιώματα.



12. Πολιτική Κυβερνοασφάλειας

Η προστασία των πληροφοριακών συστημάτων του Νοσοκομείου αποτελεί απαραίτητη προϋπόθεση για την ασφαλή και απρόσκοπτη λειτουργία των υπηρεσιών υγείας, καθώς και για την προστασία των δεδομένων προσωπικού χαρακτήρα που διαχειρίζεται ο οργανισμός.

Η Πολιτική Κυβερνοασφάλειας έχει ως βασικούς στόχους:

- τη διασφάλιση της εμπιστευτικότητας των πληροφοριών,
- την προστασία της ακεραιότητας των δεδομένων,
- τη διατήρηση της διαθεσιμότητας των πληροφοριακών συστημάτων.

Για την επίτευξη των παραπάνω στόχων εφαρμόζονται κατάλληλα τεχνικά και οργανωτικά μέτρα ασφάλειας, στα οποία ενδεικτικά περιλαμβάνονται:

- η χρήση συστημάτων προστασίας δικτύου syzefxis (firewalls),
- η αξιοποίηση συστημάτων ανίχνευσης και αποτροπής επιθέσεων,
- η χρήση κατάλληλου λογισμικού προστασίας από κακόβουλο λογισμικό,
- η τακτική ενημέρωση του λογισμικού και των λειτουργικών συστημάτων,
- ο έλεγχος και η διαχείριση της πρόσβασης των χρηστών,
- η καταγραφή και παρακολούθηση συμβάντων που σχετίζονται με την ασφάλεια.

Το Αυτοτελές Τμήμα Οργάνωσης και Πληροφορικής είναι αρμόδιο για την εφαρμογή των προβλεπόμενων μέτρων κυβερνοασφάλειας, καθώς και για την παρακολούθηση της ορθής και ασφαλούς λειτουργίας των πληροφοριακών συστημάτων.

13. Διαχείριση Περιστατικών Ασφάλειας Πληροφοριών

Ως περιστατικό ασφάλειας πληροφοριών νοείται κάθε συμβάν που μπορεί να επηρεάσει ή να θέσει σε κίνδυνο την ασφάλεια, την ακεραιότητα ή τη διαθεσιμότητα των πληροφοριακών συστημάτων.

Ενδεικτικά, ως περιστατικά ασφάλειας μπορεί να θεωρηθούν:

- μη εξουσιοδοτημένη πρόσβαση σε πληροφοριακά συστήματα,
- απώλεια, αλλοίωση ή διαγραφή δεδομένων,
- προσβολή ή μόλυνση συστημάτων από κακόβουλο λογισμικό,
- επιθέσεις ransomware,
- υποκλοπή ή παραβίαση κωδικών πρόσβασης.



Σε περίπτωση που ένας χρήστης αντιληφθεί ή υποψιαστεί πιθανό περιστατικό ασφάλειας, οφείλει να ενημερώσει άμεσα το Αυτοτελές Τμήμα Οργάνωσης και Πληροφορικής.

Η διαδικασία διαχείρισης ενός περιστατικού περιλαμβάνει:

1. την καταγραφή και τεκμηρίωση του περιστατικού,
2. την αξιολόγηση της σοβαρότητας και της έκτασής του,
3. τη λήψη μέτρων για τον περιορισμό των επιπτώσεων,
4. την αποκατάσταση της ομαλής λειτουργίας των επηρεαζόμενων συστημάτων.
5. τη διερεύνηση και τον προσδιορισμό των αιτιών που προκάλεσαν το περιστατικό,
6. τη λήψη των κατάλληλων διορθωτικών μέτρων, ώστε να αντιμετωπιστούν οι αιτίες και να περιοριστεί η πιθανότητα επανάληψής του.

14. Διαχείριση Κακόβουλου Λογισμικού

Το Νοσοκομείο εφαρμόζει μέτρα προστασίας από κακόβουλο λογισμικό, με σκοπό την πρόληψη και αντιμετώπιση μολύνσεων από ιούς, trojans, ransomware και άλλες μορφές κακόβουλων απειλών.

Για τον σκοπό αυτό:

- εγκαθίσταται κατάλληλο λογισμικό προστασίας από κακόβουλο λογισμικό σε όλους τους σταθμούς εργασίας και στους εξυπηρετητές,
- πραγματοποιούνται σε τακτική βάση οι απαιτούμενες ενημερώσεις των συστημάτων και των βάσεων δεδομένων προστασίας,
- εφαρμόζονται πολιτικές και μηχανισμοί ελέγχου των αρχείων και των συνημμένων που διακινούνται μέσω ηλεκτρονικού ταχυδρομείου.

Σε περίπτωση εντοπισμού ή υποψίας ύπαρξης κακόβουλου λογισμικού:

- το επηρεαζόμενο σύστημα αποσυνδέεται από το δίκτυο,
- πραγματοποιείται έλεγχος από το Αυτοτελές Τμήμα Οργάνωσης και Πληροφορικής,
- λαμβάνονται άμεσα τα απαραίτητα μέτρα για την αντιμετώπιση του περιστατικού και την αποκατάσταση της ασφαλούς λειτουργίας του συστήματος.

15. Διαχείριση Επιθέσεων Ηλεκτρονικού Ψαρέματος (Phishing)

Οι επιθέσεις ηλεκτρονικού ψαρέματος (phishing) αποτελούν μία από τις συχνότερες απειλές για την ασφάλεια των πληροφοριακών συστημάτων.



Οι χρήστες πρέπει να επιδεικνύουν αυξημένη προσοχή κατά τη διαχείριση μηνυμάτων ηλεκτρονικού ταχυδρομείου τα οποία:

- ζητούν την εισαγωγή ή γνωστοποίηση κωδικών πρόσβασης,
- ζητούν προσωπικά ή άλλα εμπιστευτικά στοιχεία,
- περιέχουν συνδέσμους που παραπέμπουν σε άγνωστες ή ύποπτες ιστοσελίδες,
- περιλαμβάνουν ύποπτα ή μη αναμενόμενα συνημμένα αρχεία.

Σε περίπτωση υποψίας ότι ένα μήνυμα αποτελεί απόπειρα phishing:

- το μήνυμα δεν πρέπει να ανοίγεται,
- δεν πρέπει να επιλέγονται ή να ενεργοποιούνται οι σύνδεσμοι που περιλαμβάνει,
- το μήνυμα πρέπει να προωθείται άμεσα στο Αυτοτελές Τμήμα Οργάνωσης και Πληροφορικής για έλεγχο.

16. Αντίγραφα Ασφαλείας και Ανάκτηση Δεδομένων

Το Νοσοκομείο εφαρμόζει διαδικασίες δημιουργίας και διαχείρισης αντιγράφων ασφαλείας, με σκοπό την προστασία των κρίσιμων πληροφοριακών δεδομένων και τη δυνατότητα ανάκτησής τους όταν απαιτείται.

Τα αντίγραφα ασφαλείας:

- δημιουργούνται σε προκαθορισμένα και τακτά χρονικά διαστήματα,
- αποθηκεύονται σε κατάλληλους και ασφαλείς αποθηκευτικούς χώρους,
- προστατεύονται από πρόσβαση μη εξουσιοδοτημένων προσώπων.

Παράλληλα, πραγματοποιούνται περιοδικοί έλεγχοι και δοκιμές αποκατάστασης των δεδομένων, ώστε να επιβεβαιώνεται ότι τα αντίγραφα ασφαλείας είναι λειτουργικά και μπορούν να χρησιμοποιηθούν αποτελεσματικά σε περίπτωση ανάγκης.

17. Σχέδιο Ανάκαμψης από Καταστροφή (Disaster Recovery)

Το Νοσοκομείο διαθέτει σχέδιο ανάκαμψης από καταστροφή, με στόχο την αποκατάσταση της λειτουργίας των πληροφοριακών συστημάτων σε περίπτωση σοβαρού τεχνικού προβλήματος, εκτεταμένης βλάβης ή άλλου περιστατικού που επηρεάζει τη λειτουργία τους.

Το σχέδιο ανάκαμψης από καταστροφή περιλαμβάνει διαδικασίες που αφορούν:

- την αποκατάσταση των κρίσιμων πληροφοριακών συστημάτων,



- την επαναφορά των δεδομένων μέσω των διαθέσιμων αντιγράφων ασφαλείας,
- τη διασφάλιση της συνέχειας των βασικών λειτουργιών και υπηρεσιών του Νοσοκομείου.

18. Κυρώσεις

Η μη συμμόρφωση με τους κανόνες και τις απαιτήσεις που προβλέπονται στον παρόντα κανονισμό ενδέχεται να επιφέρει τις προβλεπόμενες πειθαρχικές ή άλλες νόμιμες συνέπειες.

Ανάλογα με τη φύση και τη σοβαρότητα της παράβασης, μπορεί να επιβληθούν:

- περιορισμός, προσωρινή αναστολή ή ανάκληση των δικαιωμάτων πρόσβασης σε πληροφοριακά συστήματα,
- πειθαρχικές κυρώσεις σύμφωνα με τις διατάξεις του ισχύοντος κανονισμού προσωπικού,
- νομικές ενέργειες, όπου αυτό προβλέπεται από την ισχύουσα νομοθεσία.

19. Αναθεώρηση Κανονισμού

Ο παρών κανονισμός επανεξετάζεται και επικαιροποιείται σε τακτά χρονικά διαστήματα από το Αυτοτελές Τμήμα Οργάνωσης και Πληροφορικής, σε συνεργασία με τη Διοίκηση του Νοσοκομείου.

Η αναθεώρησή του πραγματοποιείται ιδίως:

- όταν προκύπτουν νέες τεχνολογικές απαιτήσεις ή σημαντικές αλλαγές στις πληροφοριακές υποδομές,
- όταν μεταβάλλεται το ισχύον νομοθετικό και κανονιστικό πλαίσιο,
- όταν από την αξιολόγηση της εφαρμογής του διαπιστώνεται ανάγκη βελτίωσης ή ενίσχυσης των διαδικασιών και των μέτρων ασφάλειας.



ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ
ΠΑΙΔΩΝ ΠΑΤΡΩΝ
«ΚΑΡΑΜΑΝΔΑΝΕΙΟ»

ΑΛΓΟΡΙΘΜΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΚΑΙ ΧΡΗΣΗΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Έκδοση: 1.0
Ημ/νία: 2026
Σελίδα: 1 από 1

ΡΟΛΟΙ ΚΑΙ ΑΡΜΟΔΙΟΤΗΤΕΣ

ΧΡΗΣΤΗΣ / ΑΙΤΩΝ

- Υποβάλλει αίτηση πρόσβασης.
- Χρησιμοποιεί τα συστήματα σύμφωνα με τον Κανονισμό.
- Ενημερώνει για κάθε ύποπτο συμβάν ή παραβίαση.

ΥΠΕΥΘΥΝΟΣ ΑΥΤΟΤΕΛΟΥΣ ΤΜΗΜΑΤΟΣ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

- Ελέγχει την αναγκαιότητα και το εύρος της πρόσβασης.
- Εισηγείται έγκριση ή απόρριψη της αίτησης.

ΑΥΤΟΤΕΛΕΣ ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

- Ελέγχει και αξιολογεί αιτήματα.
- Δημιουργεί / τροποποιεί λογαριασμούς και δικαιώματα.
- Παρακολουθεί, καταγράφει και προστατεύει τα συστήματα.
- Διαχειρίζεται περιστατικά ασφάλειας.

ΟΛΟΙ ΟΙ ΧΡΗΣΤΕΣ

- Τηρούν την Πολιτική Ασφάλειας και τον Κανονισμό.
- Προστατεύουν δεδομένα και κωδικούς πρόσβασης.
- Χρησιμοποιούν τα συστήματα αποκλειστικά για υπηρεσιακούς σκοπούς.

ΔΙΟΙΚΗΣΗ

- Εγκρίνει πολιτικές και διαδικασίες.
- Παρέχει τους απαραίτητους πόρους.
- Υποστηρίζει τη συμμόρφωση και τη βελτίωση των διαδικασιών.

1 ΕΝΑΡΞΗ ΑΝΑΓΚΗΣ ΠΡΟΣΒΑΣΗΣ

Προκύπτει ανάγκη πρόσβασης εργαζομένου σε πληροφοριακό σύστημα;

ΟΧΙ

ΤΕΛΟΣ
ΔΙΑΔΙΚΑΣΙΑΣ

ΝΑΙ

2 ΥΠΟΒΟΛΗ ΑΙΤΗΣΗΣ

Υποβάλλεται η «Αίτηση Χορήγησης Πρόσβασης Νέου Χρήστη» με στοιχεία χρήστη, σύστημα/τα, επίπεδο πρόσβασης και ειδικές ανάγκες.

3 ΕΛΕΓΧΟΣ ΑΠΟ ΥΠΕΥΘΥΝΟ ΑΥΤΟΤΕΛΟΥΣ ΤΜΗΜΑΤΟΣ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ελέγχεται η αναγκαιότητα, ο ρόλος και το εύρος των δικαιωμάτων πρόσβασης.

ΟΧΙ

ΑΠΟΡΡΙΨΗ
ΑΙΤΗΣΗΣ

ΝΑΙ

4 ΕΛΕΓΧΟΣ ΑΠΟ ΑΥΤΟΤΕΛΕΣ ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

Έλεγχος πληρότητας, τεχνικής δυνατότητας, επιπέδου δικαιωμάτων, συμβατότητας με Πολιτική Ασφάλειας και ανάγκης δημιουργίας/τροποποίησης λογαριασμού.

ΟΧΙ

ΔΙΟΡΘΩΣΗ
Ή
ΑΠΟΡΡΙΨΗ

ΝΑΙ

5 ΔΗΜΙΟΥΡΓΙΑ / ΕΝΕΡΓΟΠΟΙΗΣΗ ΠΡΟΣΒΑΣΗΣ

- Δημιουργία ή ενεργοποίηση λογαριασμού χρήστη.
- Απόδοση μοναδικών στοιχείων πρόσβασης.
- Καθορισμός δικαιωμάτων σύμφωνα με την αρχή της ελάχιστης αναγκαίας πρόσβασης.
- Ενεργοποίηση πρόσβασης στα εγκεκριμένα συστήματα.
- Ειδικά για DocuTracks: ηλεκτρονική διακίνηση εγγράφων, πρωτοκόλληση, διαχείριση φακέλων/ρώων εργασίας, ανάλογα με τον ρόλο.

6 ΕΝΗΜΕΡΩΣΗ ΚΑΙ ΑΠΟΔΟΧΗ ΥΠΟΧΡΕΩΣΕΩΝ ΧΡΗΣΤΗ

Ο χρήστης ενημερώνεται για κανόνες χρήσης, κωδικούς, προστασία δεδομένων, μη εγκατάσταση λογισμικού, μη εγκεκριμένα μέσα αποθήκευσης και άμεση αναφορά ύποπτων συμβάντων.

7 ΚΑΝΟΝΙΚΗ ΧΡΗΣΗ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Ο χρήστης συνδέεται με προσωπικό λογαριασμό και χρησιμοποιεί μόνο εγκεκριμένα συστήματα και δεδομένα για υπηρεσιακούς σκοπούς.

8 ΔΙΑΠΙΣΤΩΝΕΤΑΙ ΤΕΧΝΙΚΟ ΠΡΟΒΛΗΜΑ Ή ΠΕΡΙΣΤΑΤΙΚΟ ΑΣΦΑΛΕΙΑΣ;

ΟΧΙ

ΝΑΙ

9 ΔΙΑΧΕΙΡΙΣΗ ΠΕΡΙΣΤΑΤΙΚΟΥ

- Καταγραφή
- Αξιολόγηση
- Περιορισμός επιπτώσεων
- Αποκατάσταση
- Διερεύνηση
- Διορθωτικά μέτρα

10 ΜΕΤΑΒΟΛΗ ΡΟΛΟΥ / ΥΠΗΡΕΣΙΑΚΗΣ ΚΑΤΑΣΤΑΣΗΣ;

ΟΧΙ

ΝΑΙ

11 ΤΡΟΠΟΠΟΙΗΣΗ ΔΙΚΑΙΩΜΑΤΩΝ

Ενημέρωση Αυτοτελούς Τμήματος Οργάνωσης και Πληροφορικής για προσθήκη, περιορισμό ή ανάκληση δικαιωμάτων πρόσβασης.

12 ΛΗΞΗ ΣΥΝΕΡΓΑΣΙΑΣ;

ΟΧΙ

ΝΑΙ

13 ΑΝΑΚΛΗΣΗ ΠΡΟΣΒΑΣΗΣ

- Απενεργοποίηση λογαριασμού
- Ανάκληση δικαιωμάτων
- Διακοπή VPN / απομακρυσμένης πρόσβασης
- Αφαίρεση πρόσβασης

ΤΕΛΟΣ ΔΙΑΔΙΚΑΣΙΑΣ

ΚΥΡΙΕΣ ΑΡΧΕΣ ΛΕΙΤΟΥΡΓΙΑΣ

- Εμπιστευτικότητα
- Ακεραιότητα
- Διαθεσιμότητα
- Λογοδοσία
- Ελάχιστη αναγκαία πρόσβαση
- Συμμόρφωση με τη νομοθεσία, τον GDPR, τις πολιτικές και τον κανονισμό

ΑΠΑΓΟΡΕΥΕΤΑΙ

- Χρήση για μη υπηρεσιακούς σκοπούς
- Κοινοποίηση κωδικών πρόσβασης
- Εγκατάσταση μη εγκεκριμένου λογισμικού
- Χρήση μη εγκεκριμένων μέσων αποθήκευσης
- Αποθήκευση δεδομένων υγείας σε προσωπικές συσκευές
- Μη εξουσιοδοτημένη διακίνηση ή αποκάλυψη πληροφοριών

ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

- Ασκληπιός – Patient
- Ασκληπιός – Finance
- Ιατρονοσηλευτικό Σύστημα
- RIS – PACS
- LIS
- Σύστημα Χειρουργείου
- DocuTracks – Ηλεκτρονική Διακίνηση Εγγράφων
- Λοιπά πληροφοριακά συστήματα

ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

- Κανονισμός Λειτουργίας Πληροφοριακών Συστημάτων
- Πολιτική Ασφάλειας
- Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)
- Εθνική νομοθεσία περί προστασίας δεδομένων
- Κανονισμός Προσωπικού Νοσοκομείου

Γ.Ν.Π.Π. «ΚΑΡΑΜΑΝΔΑΝΕΙΟ»
Αυτοτελές Τμήμα Οργάνωσης και Πληροφορικής

ΣΗΜΕΙΩΣΗ: Ο παρών αλγόριθμος εφαρμόζεται σε όλες τις περιπτώσεις πρόσβασης, χρήσης, τροποποίησης και ανάκλησης δικαιωμάτων στα πληροφοριακά συστήματα του Νοσοκομείου.



Η ΔΙΟΙΚΗΤΡΙΑ ΤΟΥ ΝΟΣΟΚΟΜΕΙΟΥ



Ο ΥΠΕΥΘΥΝΟΣ ΤΟΥ ΑΥΤΟΤΕΛΟΥΣ
ΤΜΗΜΑΤΟΣ
ΟΡΓΑΝΩΣΗΣ & ΠΛΗΡΟΦΟΡΙΚΗΣ

ΤΖΩΡΤΖΗΣ ΓΕΩΡΓΙΟΣ

(ΥΠΟΓΡΑΦΗ)