

ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΕΚΔΟΣΗ 2 | 29 Σεπτεμβρίου 2025
Απόφαση ΔΣ 904/29-09-2025

ΟΜΙΛΟΣ ΙΑΤΡΙΚΟΥ ΑΘΗΝΩΝ

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ – ΣΚΟΠΟΣ ΚΑΙ ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ 3
2. ΝΟΜΟΘΕΤΙΚΟ ΚΑΙ ΚΑΝΟΝΙΣΤΙΚΟ ΠΛΑΙΣΙΟ 3
3. ΟΡΓΑΝΩΤΙΚΗ ΔΟΜΗ ΚΑΙ ΡΟΛΟΙ 4
4. ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΣΤΡΑΤΗΓΙΚΟΙ ΣΤΟΧΟΙ 5
5. ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 5
6. ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΑΙ ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΣΥΝΕΧΕΙΑ 6
7. ΕΚΠΑΙΔΕΥΣΗ, ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΚΑΙ ΚΟΥΛΤΟΥΡΑ ΑΣΦΑΛΕΙΑΣ 7
8. ΣΥΝΕΡΓΑΤΕΣ, ΠΡΟΜΗΘΕΥΤΕΣ ΚΑΙ ΤΡΙΤΟΙ ΦΟΡΕΙΣ 7
9. ΣΥΝΕΧΗΣ ΒΕΛΤΙΩΣΗ ΚΑΙ ΑΝΑΘΕΩΡΗΣΗ ΤΗΣ ΠΟΛΙΤΙΚΗΣ 8
10. ΔΕΣΜΕΥΣΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΚΑΤΑΛΗΚΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ 9
ΠΑΡΑΡΤΗΜΑ Ι: ΙΣΤΟΡΙΚΟ ΕΓΓΡΑΦΟΥ 10

1. ΕΙΣΑΓΩΓΗ – ΣΚΟΠΟΣ ΚΑΙ ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η ασφάλεια των πληροφοριών και η προστασία των προσωπικών δεδομένων αποτελούν αδιαπραγμάτευτη προϋπόθεση για την παροχή υπηρεσιών υγείας υψηλής ποιότητας. Η Εταιρεία «ΙΑΤΡΙΚΟ ΑΘΗΝΩΝ Ε.Α.Ε.» και οι θυγατρικές της που αποτελούν τον Όμιλο Ιατρικού Αθηνών, (στην συνέχεια «Όμιλος») αναγνωρίζοντας την ευθύνη τους απέναντι στους ασθενείς, τους εργαζόμενους και τους συνεργάτες του, υιοθετεί την παρούσα Πολιτική Ασφάλειας Πληροφοριών και Κυβερνοασφάλειας, η οποία αποτελεί επίσημη δέσμευση της Διοίκησης και ενιαίο σημείο αναφοράς για όλα τα θέματα που αφορούν την ασφάλεια και την προστασία των δεδομένων.

Η Πολιτική αυτή:

- Εκφράζει τη στρατηγική δέσμευση του Ομίλου στην προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.
- Συμμορφώνεται με την ισχύουσα ευρωπαϊκή και εθνική νομοθεσία (Οδηγία NIS2, ν. 5160/2024, ΚΥΑ 1689/2025, GDPR) και με τα διεθνή πρότυπα (ISO 27001, ISO 22301).
- Αντικαθιστά την προηγούμενη Πολιτική Ασφάλειας Πληροφοριών (έκδοση 2023) του Ομίλου διασυνδέοντας με τις επιμέρους διεργασίες Δ.Ο.10 (Διαχείριση Ιατρικών Δεδομένων) και Δ.Ο.11 (Διαχείριση Τεχνολογίας Υγείας και Πληροφοριακών Συστημάτων) του Συστήματος Διαχείρισης Ποιότητας και αποτελεί το επίσημο σημείο αναφοράς για όλα τα θέματα κυβερνοασφάλειας.

Πεδίο Εφαρμογής

Η Πολιτική Ασφάλειας Πληροφοριών και Κυβερνοασφάλειας καλύπτει:

- Όλες τις Μονάδες Υγείας του Ομίλου (νοσοκομεία, διαγνωστικά κέντρα, κλινικές).
- Τις διοικητικές και υποστηρικτικές υπηρεσίες.
- Τα πληροφοριακά συστήματα (ηλεκτρονικός φάκελος ασθενή, εργαστηριακά συστήματα, ιατρικές εικόνες, ERP, τηλεϊατρική).
- Τον ιατροτεχνολογικό εξοπλισμό που συνδέεται με δίκτυα και συστήματα πληροφορικής.
- Όλους τους εργαζόμενους, συνεργάτες, προμηθευτές και τρίτους παρόχους υπηρεσιών.
- Όλες τις μορφές πληροφορίας (ηλεκτρονική, έντυπη, προφορική).

2. ΝΟΜΟΘΕΤΙΚΟ ΚΑΙ ΚΑΝΟΝΙΣΤΙΚΟ ΠΛΑΙΣΙΟ

Ο Όμιλος Ιατρικού Αθηνών λειτουργεί σε ένα ιδιαίτερα αυστηρό κανονιστικό περιβάλλον, όπου η συμμόρφωση με τους κανόνες ασφάλειας πληροφοριών και κυβερνοασφάλειας δεν είναι επιλογή, αλλά υποχρέωση. Η παρούσα Πολιτική στηρίζεται σε τρεις βασικούς άξονες: το ευρωπαϊκό και εθνικό δίκαιο, τα διεθνή πρότυπα, και τις εσωτερικές πολιτικές του Ομίλου.

2.1 Ευρωπαϊκό και Εθνικό Πλαίσιο

- Οδηγία (ΕΕ) 2022/2555 – NIS2: Θέτει ελάχιστους κανόνες για τη διαχείριση κινδύνων κυβερνοασφάλειας και την υποχρέωση αναφοράς περιστατικών.
- Νόμος 5160/2024: Ενσωματώνει την Οδηγία NIS2 στο ελληνικό δίκαιο, ορίζοντας σαφείς υποχρεώσεις για βασικές και σημαντικές οντότητες υγείας.
- ΚΥΑ 1689/2025: Καθορίζει τα ελάχιστα τεχνικά, οργανωτικά και επιχειρησιακά μέτρα που πρέπει να εφαρμόζουν οι φορείς υγείας στην Ελλάδα.
- Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) & ν. 4624/2019: Ρυθμίζουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα και ενισχύουν τα δικαιώματα των ασθενών.
- Κανονισμός eIDAS (910/2014): Ορίζει τις απαιτήσεις για την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης.

2.2 Διεθνή Πρότυπα και Βέλτιστες Πρακτικές

- ISO/IEC 27001:2022: Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών.
- ISO 22301:2019: Επιχειρησιακή συνέχεια και διαχείριση κρίσεων.
- ISO/IEC 27701:2019: Προστασία προσωπικών δεδομένων στο πλαίσιο του ISO 27001.
- NIST Cybersecurity Framework: Οδηγός διεθνούς κύρους για risk-based διακυβέρνηση.

2.3 Κλαδικά Πρότυπα Υγείας

- JCI (Joint Commission International): Διεθνές πρότυπο ποιότητας και ασφάλειας στον χώρο της υγείας.
- HIPAA (ΗΠΑ): Χρησιμοποιείται ως σημείο αναφοράς για την προστασία δεδομένων υγείας, χωρίς νομική υποχρέωση στην Ελλάδα.
- Κατευθυντήριες Οδηγίες Υπουργείου Υγείας: Ιδιαίτερα για τον ηλεκτρονικό φάκελο ασθενή και τις υπηρεσίες eHealth.

2.4 Εσωτερικό Πλαίσιο Ομίλου

Η Πολιτική αυτή ενσωματώνει και κατευθύνει:

- Τις εσωτερικές διαδικασίες για τη διαχείριση ιατρικών δεδομένων, τεχνολογίας υγείας και πληροφοριακών συστημάτων.
- Την προηγούμενη Πολιτική Ασφάλειας Πληροφοριών (2023), η οποία αντικαθίσταται και θεωρείται πλέον ιστορική έκδοση.

3. ΟΡΓΑΝΩΤΙΚΗ ΔΟΜΗ ΚΑΙ ΡΟΛΟΙ

Η κυβερνοασφάλεια στον Όμιλο Ιατρικού Αθηνών δεν είναι υπόθεση μόνο της Διεύθυνσης Πληροφορικής· είναι ευθύνη που ξεκινά από τη Διοίκηση και διαχέεται σε κάθε επίπεδο. Για να εξασφαλιστεί η αποτελεσματική διακυβέρνηση, εφαρμόζουμε ένα σαφές πλαίσιο ρόλων και αρμοδιοτήτων.

3.1 Ρόλος της Διοίκησης

Το Διοικητικό Συμβούλιο και η Διοίκηση:

- ✓ Εγκρίνουν και εποπτεύουν την Πολιτική Ασφάλειας Πληροφοριών και Κυβερνοασφάλειας.
- ✓ Καθορίζουν το επίπεδο αποδοχής κινδύνου (risk appetite).
- ✓ Διασφαλίζουν ότι διατίθενται οι αναγκαίοι πόροι (οικονομικοί, ανθρώπινοι, τεχνολογικοί).
- ✓ Παρακολουθούν συστηματικά την πρόοδο μέσω αναφορών και δεικτών απόδοσης.

3.2 Κρίσιμοι Ρόλοι

- **Chief Information Security Officer (CISO):** Σχεδιάζει και εφαρμόζει το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών, συντονίζει την ομάδα αντιμετώπισης περιστατικών και εισηγείται βελτιωτικά μέτρα.
- **Data Protection Officer (DPO):** Ελέγχει τη συμμόρφωση με τον GDPR και λειτουργεί ως σύνδεσμος με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.
- **Ομάδα Αντιμετώπισης Περιστατικών (Incident Response Team): Ενεργοποιείται** άμεσα σε περίπτωση περιστατικού κυβερνοασφάλειας. Αποτελείται από τον CISO, τον DPO, στελέχη της Πληροφορικής, εκπρόσωπο της Διοίκησης, καθώς και ειδικούς σε νομικά και επικοινωνιακά θέματα.
- **Διεύθυνση Πληροφορικής & Ασφάλειας Δεδομένων:** Υλοποιεί τα τεχνικά μέτρα, εξασφαλίζει τη διαθεσιμότητα των κρίσιμων συστημάτων και παρακολουθεί τις υποδομές με εργαλεία ασφάλειας.
- **Διεύθυνση Ποιότητας & Κλινικής Αποτελεσματικότητας:** Ενσωματώνει δείκτες ασφάλειας στο συνολικό σύστημα ποιότητας και διενεργεί εσωτερικούς ελέγχους.
- **Ιατρικό και Νοσηλευτικό Προσωπικό:** Εφαρμόζει καθημερινά τις πολιτικές εμπιστευτικότητας και αναφέρει άμεσα ύποπτα περιστατικά.
- **Εξωτερικοί Συνεργάτες και Προμηθευτές:** Δεσμεύονται συμβατικά να τηρούν τα ίδια πρότυπα ασφάλειας με τον Όμιλο και υπόκεινται σε αξιολόγηση και έλεγχο.

3.3 Επιτροπή Κυβερνοασφάλειας

Συστήνεται ειδική Επιτροπή Κυβερνοασφάλειας με συμμετοχή εκπροσώπων της Διοίκησης, του CISO, του DPO, της Πληροφορικής, της Ποιότητας και του Νομικού Τμήματος. Η Επιτροπή συνεδριάζει σε τακτική βάση και:

1. Αξιολογεί την αποτελεσματικότητα των μέτρων.
2. Εγκρίνει πλάνα βελτίωσης.
3. Υποβάλλει εισηγήσεις στο Διοικητικό Συμβούλιο.

4. ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΣΤΡΑΤΗΓΙΚΟΙ ΣΤΟΧΟΙ

Η ασφάλεια πληροφοριών στον Όμιλο Ιατρικού Αθηνών δεν είναι απλώς ένα τεχνικό μέτρο· είναι βασική αξία που διασφαλίζει την εμπιστοσύνη των ασθενών και των συνεργατών μας. Στηρίζεται σε διεθνώς αναγνωρισμένες αρχές και συγκεκριμένους στρατηγικούς στόχους.

4.1 Θεμελιώδεις Αρχές

- □ Εμπιστευτικότητα: Πρόσβαση στα δεδομένα έχουν αποκλειστικά εξουσιοδοτημένα άτομα.
- □ Ακεραιότητα: Τα δεδομένα παραμένουν πλήρη, ακριβή και αμετάβλητα.
- □ Διαθεσιμότητα: Οι κρίσιμες υπηρεσίες υγείας (π.χ. ηλεκτρονικός φάκελος ασθενή, τηλεϊατρική) παραμένουν προσβάσιμες χωρίς διακοπές.
- □ Λογοδοσία: Όλες οι ενέργειες καταγράφονται και μπορούν να ελεγχθούν.
- □ Αναλογικότητα: Τα μέτρα προσαρμόζονται στη σοβαρότητα των κινδύνων και στη φύση των δεδομένων, όπως απαιτεί η νομοθεσία.
- □ Συνεχής Βελτίωση: Η πολιτική επανεξετάζεται τακτικά, ώστε να ενσωματώνει νέες απειλές, τεχνολογίες και βέλτιστες πρακτικές.

4.2 Στρατηγικοί Στόχοι

1. **Κανονιστική Συμμόρφωση:** Διασφάλιση πλήρους συμμόρφωσης με την Οδηγία NIS2, τον ν. 5160/2024, την ΚΥΑ 1689/2025, τον GDPR και τα διεθνή πρότυπα ISO.
2. **Προστασία Δεδομένων Υγείας:** Διαφύλαξη της εμπιστευτικότητας και της ιδιωτικότητας των ασθενών, με μηδενική ανοχή σε παραβιάσεις.
3. **Κυβερνοανθεκτικότητα:** Εξασφάλιση ότι ο Όμιλος παραμένει λειτουργικός ακόμη και σε συνθήκες κυβερνοεπίθεσης ή κρίσης, μέσω σχεδίων αποκατάστασης και επιχειρησιακής συνέχειας.
4. **Ασφάλεια ως Κουλτούρα:** Ενίσχυση της συνείδησης όλων των εργαζομένων μέσω εκπαιδεύσεων και συνεχούς ενημέρωσης, ώστε η ασφάλεια να αποτελεί μέρος της καθημερινής πρακτικής.
5. **Διαχείριση Κινδύνων:** Εφαρμογή συστηματικής αξιολόγησης κινδύνων και λήψη μέτρων που μειώνουν τις πιθανότητες και τις επιπτώσεις περιστατικών ασφάλειας.
6. **Διαφάνεια και Εμπιστοσύνη:** Ενίσχυση της εμπιστοσύνης ασθενών και συνεργατών μέσω υπεύθυνης και σαφούς επικοινωνίας σε ζητήματα ασφάλειας.

5. ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Η ασφάλεια πληροφοριών δεν είναι στατική· αποτελεί μια συνεχώς εξελισσόμενη διαδικασία. Ο Όμιλος Ιατρικού Αθηνών εφαρμόζει ένα ολοκληρωμένο πλαίσιο διαχείρισης κινδύνων, σύμφωνα με την Οδηγία NIS2, την ΚΥΑ 1689/2025 και τα διεθνή πρότυπα ISO 27005 και ISO 31000.

5.1 Στρατηγική Διαχείρισης Κινδύνων

- ✓ Αναγνωρίζουμε ότι οι κίνδυνοι μπορεί να είναι τεχνικοί (π.χ. κακόβουλο λογισμικό), επιχειρησιακοί (π.χ. διακοπή κρίσιμης υπηρεσίας), κανονιστικοί (π.χ. παραβίαση GDPR) ή να προέρχονται από τρίτους συνεργάτες.
- ✓ Υιοθετούμε risk-based προσέγγιση: κάθε σύστημα, δεδομένο ή συνεργάτης αξιολογείται ως προς την πιθανότητα και τον αντίκτυπο ενός περιστατικού.

- ✓ Το επίπεδο αποδοχής κινδύνου (risk appetite) ορίζεται από τη Διοίκηση και επανεξετάζεται ετησίως.

5.2 Διαδικασία Εκτίμησης Κινδύνων

Η διαδικασία περιλαμβάνει:

1. Αναγνώριση κρίσιμων στοιχείων (πληροφοριακά συστήματα, ιατρικά δεδομένα, τεχνολογικός εξοπλισμός).
2. Εντοπισμό απειλών και ευπαθειών (π.χ. ransomware, phishing, ανθρώπινα λάθη, κλιματική κρίση, φυσικές καταστροφές).
3. Ανάλυση επιχειρησιακών επιπτώσεων (Business Impact Analysis): εκτίμηση των συνεπειών σε περίπτωση διακοπής.
4. Αξιολόγηση πιθανότητας και σοβαρότητας: κατηγοριοποίηση των κινδύνων σε επίπεδα (χαμηλό, μεσαίο, υψηλό).
5. Κατάρτιση Σχεδίου Αντιμετώπισης: επιλογή προληπτικών ή διορθωτικών μέτρων, με βάση κόστος/όφελος και κανονιστικές απαιτήσεις.

Κατηγορίες Κινδύνων

- ✓ Τεχνολογικοί: επιθέσεις κακόβουλου λογισμικού, απώλεια δεδομένων, αποτυχία συστημάτων.
- ✓ Ανθρώπινοι: λάθη χρηστών, ελλιπής εκπαίδευση, κακόβουλη ενέργεια εκ των έσω.
- ✓ Φυσικοί: πυρκαγιά, σεισμός, πλημμύρα.
- ✓ Συνεργατών: ανεπαρκή μέτρα ασφάλειας από προμηθευτές ή συνεργάτες.
- ✓ Κανονιστικοί / Νομικοί: παραβίαση υποχρεώσεων NIS2 ή GDPR.
- ✓ Μέτρα Μείωσης Κινδύνων

Για κάθε αναγνωρισμένο κίνδυνο επιλέγονται κατάλληλα μέτρα, όπως:

- ✓ Τεχνικές λύσεις (firewalls, κρυπτογράφηση, έλεγχος πρόσβασης).
- ✓ Οργανωτικά μέτρα (πολιτικές, συμβάσεις με συνεργάτες, διαδικασίες).
- ✓ Εκπαίδευση προσωπικού και προγράμματα ευαισθητοποίησης.
- ✓ Σχέδια αποκατάστασης (Disaster Recovery Plan) και επιχειρησιακής συνέχειας (Business Continuity Plan).

6. ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΑΙ ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΣΥΝΕΧΕΙΑ

Παρά τα ισχυρά προληπτικά μέτρα, κανένα σύστημα δεν είναι απολύτως άτρωτο. Ο Όμιλος Ιατρικού Αθηνών αναγνωρίζει ότι μπορεί να προκύψουν περιστατικά κυβερνοασφάλειας ή διακοπές λειτουργίας και έχει θεσπίσει διαδικασίες για την άμεση και αποτελεσματική διαχείρισή τους.

6.1 Αντιμετώπιση Περιστατικών (Incident Response)

- ✓ Έχει συσταθεί Ομάδα Αντιμετώπισης Περιστατικών (Incident Response Team – IRT), με επικεφαλής τον CISO και μέλη από το DPO, το Τμήμα Πληροφορικής, τη Διοίκηση, το Νομικό και την Επικοινωνία.
- ✓ Η Ομάδα ενεργοποιείται αμέσως με την ανίχνευση περιστατικού (π.χ. κυβερνοεπίθεση, απώλεια δεδομένων).
- ✓ Προτεραιότητα δίνεται στον περιορισμό της ζημιάς, στην προστασία των ασθενών και στην αποκατάσταση της λειτουργίας.
- ✓ Όπου απαιτείται, γίνονται αναφορές στις αρμόδιες αρχές εντός των προβλεπόμενων προθεσμιών (24 ώρες για NIS2, 72 ώρες για GDPR).
- ✓ Όλα τα περιστατικά καταγράφονται και αναλύονται ώστε να εξαχθούν διδάγματα και να βελτιωθούν οι διαδικασίες.

6.2 Επιχειρησιακή Συνέχεια

Ο Όμιλος εφαρμόζει Σχέδιο Επιχειρησιακής Συνέχειας (Business Continuity Plan – BCP) και Σχέδιο Αποκατάστασης από Καταστροφή (Disaster Recovery Plan – DRP), τα οποία:

- ✓ Εξασφαλίζουν την απρόσκοπτη λειτουργία κρίσιμων συστημάτων (όπως ο ηλεκτρονικός φάκελος ασθενή).

- ✓ Ορίζουν εναλλακτικές λύσεις και διαδικασίες σε περίπτωση σοβαρής διακοπής.
- ✓ Περιλαμβάνουν στόχους χρόνου αποκατάστασης (Recovery Time Objectives – RTO) και στόχους απώλειας δεδομένων (Recovery Point Objectives – RPO), με σαφείς δεσμεύσεις διαθεσιμότητας.
- ✓ Δοκιμάζονται σε τακτική βάση μέσω ασκήσεων προσομοίωσης.

6.3 Επικοινωνία και Διαφάνεια

Σε περίπτωση περιστατικού που επηρεάζει ασθενείς ή συνεργάτες:

- ✓ Ο Όμιλος ενημερώνει άμεσα με τρόπο σαφή και κατανοητό.
- ✓ Παρέχει οδηγίες για τυχόν ενέργειες που χρειάζεται να ακολουθήσουν οι ενδιαφερόμενοι.
- ✓ Ενισχύει την εμπιστοσύνη με διαφανή επικοινωνία και συνεργασία με τις αρμόδιες αρχές.

7. ΕΚΠΑΙΔΕΥΣΗ, ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΚΑΙ ΚΟΥΛΤΟΥΡΑ ΑΣΦΑΛΕΙΑΣ

Η κυβερνοασφάλεια δεν εξαρτάται μόνο από συστήματα και διαδικασίες· βασίζεται κυρίως στη συμπεριφορά των ανθρώπων. Ο Όμιλος Ιατρικού Αθηνών επενδύει στην εκπαίδευση και στην καλλιέργεια μιας κουλτούρας ασφάλειας που διαπερνά όλο τον οργανισμό.

7.1 Υποχρεωτική Εκπαίδευση

- ✓ Όλοι οι εργαζόμενοι, από το ιατρικό και νοσηλευτικό προσωπικό έως το διοικητικό και τεχνικό προσωπικό, συμμετέχουν σε υποχρεωτικά προγράμματα εκπαίδευσης για την ασφάλεια πληροφοριών.
- ✓ Τα προγράμματα καλύπτουν θέματα όπως: αναγνώριση ύποπτων emails (phishing), ασφαλής χρήση κωδικών, προστασία ιατρικών δεδομένων, κανόνες εμπιστευτικότητας.
- ✓ Η εκπαίδευση επαναλαμβάνεται σε ετήσια βάση και προσαρμόζεται στις νέες απειλές.

7.2 Ευαισθητοποίηση και Ενημέρωση

- ✓ Διοργανώνονται τακτικές καμπάνιες ευαισθητοποίησης για την ενίσχυση της "ασφάλειας στην πράξη".
- ✓ Διατίθεται εσωτερικό ενημερωτικό υλικό (οδηγοί, ενημερωτικά δελτία, newsletters) με πρακτικές συμβουλές.
- ✓ Ο Όμιλος ενθαρρύνει τη διαρκή επικοινωνία: κάθε εργαζόμενος μπορεί και πρέπει να αναφέρει άμεσα ύποπτα περιστατικά.

7.3 Καλλιέργεια Κουλτούρας Ασφάλειας

- ✓ Η ασφάλεια αντιμετωπίζεται όχι ως εμπόδιο, αλλά ως θεμέλιο της ποιότητας στην υγεία.
- ✓ Η συμμετοχή του προσωπικού είναι καθοριστική: η συμμόρφωση με τους κανόνες και η υπεύθυνη χρήση των συστημάτων ενισχύουν την ανθεκτικότητα του Ομίλου.
- ✓ Η Διοίκηση επιβραβεύει την υπεύθυνη στάση και ενισχύει την αίσθηση ότι «η ασφάλεια είναι υπόθεση όλων».

8. ΣΥΝΕΡΓΑΤΕΣ, ΠΡΟΜΗΘΕΥΤΕΣ ΚΑΙ ΤΡΙΤΟΙ ΦΟΡΕΙΣ

Η κυβερνοασφάλεια δεν αφορά μόνο τα εσωτερικά συστήματα του Ομίλου Ιατρικού Αθηνών. Στον χώρο της υγείας, οι συνεργασίες με εξωτερικούς φορείς (π.χ. προμηθευτές τεχνολογίας, παρόχους υπηρεσιών πληροφορικής, συμβατικούς συνεργάτες) είναι κρίσιμες και μπορεί να επηρεάσουν άμεσα την ασφάλεια των δεδομένων και των συστημάτων.

8.1 Συμβατικές Υποχρεώσεις

- ✓ Όλοι οι εξωτερικοί συνεργάτες και προμηθευτές υπογράφουν συμβάσεις που περιλαμβάνουν ρήτρες ασφάλειας πληροφοριών.
- ✓ Οι συμβάσεις ενσωματώνουν Συμφωνίες Επίπεδου Υπηρεσιών (SLA) και Συμφωνίες Επεξεργασίας Δεδομένων (DPA), ώστε να διασφαλίζεται η τήρηση των ίδιων προτύπων ασφάλειας που εφαρμόζει ο Όμιλος.

8.2 Αξιολόγηση και Παρακολούθηση

- ✓ Οι συνεργάτες αξιολογούνται με βάση την κρισιμότητα των υπηρεσιών τους και το επίπεδο κινδύνου που ενδέχεται να φέρουν (risk tiering).
- ✓ Πραγματοποιούνται τακτικοί έλεγχοι (audits) για να διαπιστωθεί η συμμόρφωσή τους με τις απαιτήσεις κυβερνοασφάλειας.
- ✓ Σε περίπτωση περιστατικού που τους αφορά, έχουν την υποχρέωση να ενημερώσουν τον Όμιλο άμεσα και πάντως εντός 24 ωρών.

8.3 Κοινή Ευθύνη

Η συνεργασία με τρίτους στηρίζεται στην αρχή της κοινής ευθύνης:

- ✓ Ο Όμιλος διασφαλίζει ότι οι συνεργάτες πληρούν υψηλά πρότυπα ασφάλειας.
- ✓ Οι συνεργάτες υποχρεούνται να εφαρμόζουν ισοδύναμα μέτρα προστασίας.
- ✓ Όλοι μαζί συνθέτουν μια ενιαία αλυσίδα ασφάλειας, χωρίς αδύναμους κρίκους.

9. ΣΥΝΕΧΗΣ ΒΕΛΤΙΩΣΗ ΚΑΙ ΑΝΑΘΕΩΡΗΣΗ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

Η κυβερνοασφάλεια είναι ένα δυναμικό πεδίο, που εξελίσσεται καθημερινά με νέες απειλές, τεχνολογίες και κανονιστικές απαιτήσεις. Ο Όμιλος Ιατρικού Αθηνών αναγνωρίζει ότι η Πολιτική Ασφάλειας Πληροφοριών και Κυβερνοασφάλειας πρέπει να παραμένει επίκαιρη και αποτελεσματική.

9.1 Αρχή της Συνεχούς Βελτίωσης

- □ Η Πολιτική ενσωματώνει την αρχή "Plan – Do – Check – Act", με στόχο τον μόνιμο κύκλο βελτίωσης.
- □ Κάθε περιστατικό, έλεγχος ή αλλαγή στο περιβάλλον (τεχνολογικό ή κανονιστικό) αποτελεί αφορμή για αναθεώρηση των μέτρων.
- □ Οι δείκτες απόδοσης (KPIs) και οι δείκτες κινδύνου (KRIs) αξιολογούνται τακτικά, ώστε να προκύπτουν μετρήσιμες βελτιώσεις.

9.2 Περιοδική Αναθεώρηση

- □ Η Πολιτική επανεξετάζεται τουλάχιστον μία φορά τον χρόνο από την Επιτροπή Κυβερνοασφάλειας και εγκρίνεται εκ νέου από τη Διοίκηση.
- □ Επιπλέον, αναθεωρείται άμεσα σε περίπτωση:
    - o αλλαγών στη νομοθεσία (π.χ. νέες κανονιστικές πράξεις ή ευρωπαϊκές οδηγίες),
    - o σημαντικών τεχνολογικών εξελίξεων,
    - o σοβαρών περιστατικών κυβερνοασφάλειας.

9.3 Συμμετοχή Όλων

- □ Η βελτίωση δεν είναι υπόθεση μόνο των υπευθύνων ασφάλειας˙ είναι υπόθεση όλων.
- □ Οι εργαζόμενοι και οι συνεργάτες ενθαρρύνονται να προτείνουν βελτιώσεις και να αναφέρουν κενά ή αδυναμίες.
- □ Η Διοίκηση δεσμεύεται να λαμβάνει υπόψη τις παρατηρήσεις και να τις ενσωματώνει όπου είναι απαραίτητο.

10. ΔΕΣΜΕΥΣΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΚΑΤΑΛΗΚΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Η Διοίκηση του Ομίλου Ιατρικού Αθηνών αναγνωρίζει ότι η προστασία των πληροφοριών και η κυβερνοασφάλεια αποτελούν ουσιώδες στοιχείο της αποστολής του Ομίλου για την παροχή υπηρεσιών υγείας με ποιότητα, ασφάλεια και αξιοπιστία. Η Διοίκηση αναλαμβάνει την πλήρη ευθύνη για την εφαρμογή της παρούσας Πολιτικής και δεσμεύεται στη συνεχή ενίσχυση των μηχανισμών ασφάλειας, σύμφωνα με τις διεθνείς πρακτικές και τις κανονιστικές υποχρεώσεις.

10.1 Δέσμευση Διοίκησης

Η Διοίκηση του Ομίλου Ιατρικού Αθηνών αναγνωρίζει ότι η προστασία των πληροφοριών και η κυβερνοασφάλεια αποτελούν ουσιώδες στοιχείο της αποστολής του Ομίλου για την παροχή υπηρεσιών υγείας με ποιότητα, ασφάλεια και αξιοπιστία. Η Διοίκηση:

- φέρει την τελική ευθύνη για την εφαρμογή της παρούσας Πολιτικής,
- διασφαλίζει τη διάθεση των απαραίτητων πόρων (τεχνικών, ανθρώπινων και οικονομικών),
- εγκρίνει και εποπτεύει την υλοποίηση όλων των μέτρων κυβερνοασφάλειας,
- δεσμεύεται στη συνεχή βελτίωση και στην έγκαιρη προσαρμογή της Πολιτικής στις νέες απαιτήσεις.

10.2 Δεσμευτική Ισχύς

- Η Πολιτική αυτή είναι δεσμευτική και υποχρεωτική για όλα τα μέλη του προσωπικού, τους συνεργάτες και τους προμηθευτές του Ομίλου.
- Αποτελεί δημόσια δέσμευση προς τους ασθενείς, τους συνεργάτες και την κοινωνία ότι η ασφάλεια των πληροφοριών βρίσκεται διαρκώς στο επίκεντρο της λειτουργίας του Ομίλου.
- Με την παρούσα έκδοση καταργούνται όλες οι προηγούμενες εκδόσεις της Πολιτικής Ασφάλειας Πληροφοριών.

10.3 Δημοσιότητα και Διαφάνεια

- Η Πολιτική δημοσιεύεται στην εταιρική ιστοσελίδα του Ομίλου, ώστε να είναι προσβάσιμη από κάθε ενδιαφερόμενο.
- Αναθεωρημένες εκδόσεις της κοινοποιούνται εγκαίρως και αναρτώνται στην ίδια θέση.
- Ο Όμιλος δεσμεύεται να επικοινωνεί με σαφήνεια κάθε σημαντική αλλαγή.

ΠΑΡΑΡΤΗΜΑ Ι: ΙΣΤΟΡΙΚΟ ΕΓΓΡΑΦΟΥ

Ημερομηνία Έκδοσης / αναθεώρησης	Αριθμός Έκδοσης	Λεπτομέρειες Αλλαγών	Έγκριση	Ημερομηνία Έκδοσης Αλλαγών
21.09.2023	1η	ΕΚΔΟΣΗ	ΔΣ	21.09.2023
29.09.2025	2η	Αντικατάσταση και αλλαγές σχετικές με την Οδηγία NIS2, ν. 5160/2024, ΚΥΑ 1689/2025	ΔΣ	29.09.2025

ΕΚΔΟΣΗ 2 | 29 Σεπτεμβρίου 2025

ΟΜΙΛΟΣ ΙΑΤΡΙΚΟΥ ΑΘΗΝΩΝ

www.iatriko.gr