4ο Παραδοτέο
Νίκος Τουλκερίδης 10718 ΗΜΜΥ
Ιανουάριος 2026

ΠΟΛΙΤΙΚΗ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ & ΡΟΛΩΝ (ACCESS CONTROL POLICY)

Έκδοση: 1.0

Ημερομηνία: Ιανουάριος 2026

1. Σκοπός

Η παρούσα πολιτική ορίζει τις αρχές και διαδικασίες για τη διαχείριση της πρόσβασης στα πληροφοριακά συστήματα του οργανισμού, σύμφωνα με τις απαιτήσεις της Οδηγίας NIS 2 (Άρθρο 21) και του Ν. 5160/2024 για την εφαρμογή μέτρων διαχείρισης κινδύνων και ασφάλειας δικτύων.

2. Πεδίο Εφαρμογής

Εφαρμόζεται σε:

- **Χρήστες:** Εσωτερικοί Ιατροί (Internal Physicians), Τεχνολόγοι Ακτινολογικού (Technologists), Διοικητικό Προσωπικό (Secretariat), Εξωτερικοί Συνεργάτες (External Physicians) και Τεχνική Υποστήριξη Προμηθευτή (Vendor Support).
- **Συστήματα / Εφαρμογές:** PACS Server (10.10.20.50), RIS (Radiology Information System), MRI Console (10.10.20.20), Σταθμοί Εργασίας Ιατρών.
- **Υποδομές / Δίκτυα:** Εσωτερικό υποδίκτυο Ακτινοδιαγνωστικού (Subnet 10.10.20.0/24) και συνδέσεις VPN.

3. Αρχές Ελέγχου Πρόσβασης

- **Ελάχιστο απαιτούμενο δικαίωμα (Least Privilege):** Οι χρήστες έχουν πρόσβαση μόνο στα δεδομένα και τις εφαρμογές που είναι απολύτως απαραίτητα για την εργασία τους.
- **MFA για ευαίσθητα συστήματα: [ΝΑΙ]** / Όχι

  → Η χρήση Ελέγχου Ταυτότητας Πολλαπλών Παραγόντων (MFA) είναι υποχρεωτική για όλες τις απομακρυσμένες συνδέσεις (VPN) του Προμηθευτή (Vendor Support) και για την πρόσβαση των διαχειριστών (IT Admin) σε κρίσιμους εξυπηρετητές (PACS Server).

4. Διαδικασία Δημιουργίας / Τροποποίησης / Απενεργοποίησης Λογαριασμών

- **Αίτηση πρόσβασης:** Υποβάλλεται εγγράφως από τον Προϊστάμενο του Ακτινοδιαγνωστικού Τμήματος.
- **Έγκριση από:** Τον Υπεύθυνο Ασφαλείας (CISO / ΥΑΣΠΕ) και τη Διεύθυνση Πληροφορικής.

- **Χρόνος απενεργοποίησης μετά από αποχώρηση:** Άμεσα (εντός 24 ωρών) για απλούς χρήστες, και εντός 1 ώρας για διαχειριστές ή σε περίπτωση απόλυσης.
- **Ετήσια αναθεώρηση ρόλων: [ΝΑΙ]** / Όχι – Συχνότητα: Ετησίως (ή εκτάκτως σε αλλαγή καθηκόντων).

5. Έλεγχος Πρόσβασης σε Δεδομένα

- **Επίπεδα πρόσβασης:**
    - **Ιατροί:** Πλήρης πρόσβαση (Read/Write) σε Κλινικά Δεδομένα & Εικόνες (DICOM).
    - **Τεχνολόγοι:** Πρόσβαση λειτουργίας στον Εξοπλισμό (MRI Console) και εγγραφής στο PACS.
    - **Γραμματεία:** Πρόσβαση μόνο σε Δημογραφικά Στοιχεία (RIS) - Όχι σε Κλινικά/Εικόνες.
    - **Vendor Support:** Πρόσβαση συντήρησης (Maintenance) μόνο κατόπιν έγκρισης και με χρονικό περιορισμό.
- **Διαδικασία έγκρισης πρόσβασης σε ευαίσθητα δεδομένα:** Απαιτείται ειδική εξουσιοδότηση βάσει ρόλου (RBAC) στο Active Directory. Κάθε πρόσβαση στον ιατρικό φάκελο καταγράφεται.

6. Καταγραφή & Παρακολούθηση

- **Τι καταγράφεται (logs):** Επιτυχημένες και αποτυχημένες προσπάθειες εισόδου (Login success/failure), προσπέλαση ευαίσθητων αρχείων (Access logs), αλλαγές δικαιωμάτων χρηστών.
- **Alerting & Incident Response:** Σε περίπτωση εντοπισμού πολλαπλών διαδοχικών αποτυχημένων προσπαθειών εισόδου (π.χ. >3 προσπάθειες/λεπτό), το σύστημα παράγει **αυτόματη ειδοποίηση ασφαλείας (SIEM Alert)** προς τον Υπεύθυνο Ασφαλείας (CISO) για την άμεση διερεύνηση πιθανής επίθεσης (Brute Force)."
- **Χρόνος διατήρησης:** 12 μήνες (σύμφωνα με τις οδηγίες της Αρχής Προστασίας Δεδομένων και NIS 2).

7. Εξαιρέσεις / Ειδικές Περιπτώσεις

- **Που δεν εφαρμόζεται;**
    - Σε καταστάσεις έκτακτης ανάγκης (Emergency / Break-glass), όπου η άμεση πρόσβαση σε ιατρικά δεδομένα είναι κρίσιμη για τη ζωή του ασθενούς. Σε αυτή την περίπτωση, η πρόσβαση καταγράφεται λεπτομερώς και ελέγχεται απολογιστικά.
    - Σε Legacy συστήματα (π.χ. παλιά MRI Console) που τεχνικά δεν υποστηρίζουν κεντρική διαχείριση χρηστών (εκεί εφαρμόζονται φυσικοί περιορισμοί πρόσβασης).

ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΕΝΗΜΕΡΩΣΕΩΝ (PATCH MANAGEMENT)

Έκδοση: 1.0

Ημερομηνία: Ιανουάριος 2026

1. Σκοπός

Η παρούσα πολιτική εξασφαλίζει ότι όλα τα συστήματα (servers, endpoints, δικτυακές συσκευές κ.λπ.) ενημερώνονται εγκαίρως για την αντιμετώπιση ευπαθειών. Σκοπός είναι η μείωση της επιφάνειας επίθεσης και η συμμόρφωση με το Άρθρο 21 της Οδηγίας NIS 2 περί διαχείρισης τρωτών σημείων.

2. Πεδίο Εφαρμογής

- **Servers:** PACS Server (Windows Server 2019 / Linux), RIS Database.
- **Υπολογιστές:** Σταθμοί Εργασίας Ιατρών (Windows 10/11 Pro), Σταθμοί Γραμματείας.
- **Εξοπλισμός δικτύου:** Perimeter Firewall, Network Switches (Firmware updates).
- **Ιατροτεχνολογικός Εξοπλισμός:** MRI Console & MRI Scanner (Ειδικό καθεστώς διαχείρισης).

3. Συχνότητα Ενημερώσεων

- **Κρίσιμες ενημερώσεις (Security):**
  - **[X]** Εβδομαδιαία (Για σταθμούς εργασίας και συνήθεις servers).
  - Εντός **48** ωρών για ευπάθειες τύπου "Zero-Day" ή κρίσιμα CVEs (CVSS > 9.0).
- **Εφαρμογές (Office, Browsers):** Μηνιαία (Patch Tuesday) ή αυτόματα.
- **Λειτουργικό Σύστημα:** Μηνιαία (Quality Rollups).
- **Firmware Εξοπλισμού:** Εξαμηνιαία ή κατόπιν οδηγίας του κατασκευαστή.

4. Διαδικασία Εντοπισμού Ευπαθειών

- **Εργαλεία που χρησιμοποιούνται:** Windows Server Update Services (WSUS) για τα PC, Ειδοποιήσεις Κατασκευαστή (Vendor Bulletins) για τον MRI Scanner/PACS.
- **Πηγή ενημερώσεων:** Επίσημα αποθετήρια (Microsoft, Linux Repos), Εξουσιοδοτημένος Προμηθευτής (Vendor).

5. Διαδικασία Εφαρμογής

1. **Έλεγχος συμβατότητας:** Πριν την εγκατάσταση σε κρίσιμα συστήματα (PACS), επιβεβαιώνεται η συμβατότητα με τις ιατρικές εφαρμογές.
2. **Δοκιμή σε περιβάλλον staging:** Εφαρμογή πρώτα σε 1-2 σταθμούς εργασίας (Test Group) πριν τη μαζική διανομή.
3. **Εγκατάσταση:** Αυτοματοποιημένη (εκτός ωραρίου λειτουργίας) για τα PC. Χειροκίνητη από τον διαχειριστή για τους Servers.
4. **Rollback plan:** Διατήρηση Backup/Snapshot του συστήματος πριν την εφαρμογή κρίσιμων updates.

6. Καταγραφή

- **Σημειώνονται όλα τα patches στο:** [X] Έγγραφο Excel / Μητρώο Συντήρησης (Logbook).

7. Εξαιρέσεις / Ειδικές Περιπτώσεις (Κρίσιμο για το 3ο Παραδοτέο)

- **Σύστημα: MRI Console / MRI Scanner Workstation.**
- **Λόγος Εξαίρεσης:** Το σύστημα λειτουργεί με **Legacy OS (Windows Embedded/7)** και ιδιόκτητο λογισμικό του κατασκευαστή. Η αυτόματη ενημέρωση ενδέχεται να προκαλέσει δυσλειτουργία στον τομογράφο (Vendor Restriction).
- **Αντισταθμιστικά Μέτρα (Compensating Controls):**
    1. Το σύστημα έχει τοποθετηθεί σε **απομονωμένο VLAN (10.10.20.0/24)** χωρίς άμεση πρόσβαση στο Internet (Air-gapped logic).
    2. Αυστηροί κανόνες Firewall (Inbound/Outbound Block).
    3. Οι θύρες USB είναι κλειδωμένες για αποφυγή μόλυνσης από φυσικά μέσα.

ΠΟΛΙΤΙΚΗ ΓΙΑ DATA-AT-REST ΑΣΦΑΛΕΙΑ (ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ, ΑΚΕΡΑΙΟΤΗΤΑ, ΔΙΑΘΕΣΙΜΟΤΗΤΑ)

Έκδοση: 1.0

Ημερομηνία: Ιανουάριος 2026

1. Σκοπός

Προστασία δεδομένων που αποθηκεύονται σε servers, βάσεις δεδομένων, endpoints και αντίγραφα ασφαλείας. Στόχος είναι η αποτροπή διαρροής ιατρικών δεδομένων (PHI) και η διασφάλιση ότι οι διαγνωστικές εικόνες δεν έχουν αλλοιωθεί (Integrity).

2. Πεδίο Εφαρμογής

- **Συστήματα:** PACS Server (Αρχεία Εικόνων), Σταθμοί Εργασίας Ιατρών.
- **Βάσεις δεδομένων:** RIS Database (SQL) – Δεδομένα ασθενών και πορίσματα.
- **Αρχεία / Backups:** Τοπικά αντίγραφα ασφαλείας (NAS) και Remote Backup (Cloud/Off-site).

3. Εμπιστευτικότητα (Confidentiality)

- **Κρυπτογράφηση σε αποθήκευση: [NAI]**
    - **Αλγόριθμος: AES-256** (για τη βάση δεδομένων SQL και τα αποθηκευμένα volumes του PACS).

- **Key management:** Τα κλειδιά κρυπτογράφησης φυλάσσονται σε ξεχωριστό ασφαλή διακομιστή (Key Vault) και όχι στον ίδιο δίσκο με τα δεδομένα.
- **Πρόσβαση περιορισμένη σε χρήστες:** Μόνο εξουσιοδοτημένοι Ιατροί και ο Διαχειριστής (βάσει Active Directory Groups).

4. Ακεραιότητα (Integrity)

- **Hashing / Checksum:** Χρήση **SHA-256** checksums για κάθε αρχείο DICOM κατά την αρχειοθέτηση.
- **Logging αλλαγών αρχείων: [ΝΑΙ]**
- **Παρακολούθηση μη εξουσιοδοτημένων αλλαγών:** Χρήση εργαλείου File Integrity Monitoring (FIM) στον PACS Server. Αν αλλοιωθεί ιατρική εικόνα, παράγεται άμεσο Alert.

5. Διαθεσιμότητα (Availability)

- **Backups:**
  - **[X]** Ημερήσιο (Incremental - Τοπικά).
  - **[X]** Εβδομαδιαίο (Full - Remote Backup/Cloud).
- **Redundancy:** RAID 6 στον χώρο αποθήκευσης του PACS για ανοχή σε βλάβη 2 δίσκων ταυτόχρονα.
- **RTO (Recovery Time Objective): 4 ώρες** (Μέγιστος χρόνος επαναφοράς λειτουργίας).
- **RPO (Recovery Point Objective): 1 ώρα** (Μέγιστη επιτρεπτή απώλεια δεδομένων).

6. Εξαιρέσεις / Ειδικές Περιπτώσεις

- **Σύστημα:** MRI Console & Workstation (Local Storage).
- **Λόγος Εξαίρεσης:** Λόγω παλαιότητας του λειτουργικού συστήματος (Legacy OS - Windows Embedded) και περιορισμών του κατασκευαστή (Vendor Warranty), δεν υποστηρίζεται η κρυπτογράφηση δίσκου (π.χ. BitLocker) χωρίς κίνδυνο δυσλειτουργίας ή καθυστερήσεων στην απεικόνιση.
- **Αντισταθμιστικά Μέτρα:**
  1. **Φυσική Ασφάλεια:** Η πρόσβαση στον χώρο της Κονσόλας επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό μέσω κάρτας πρόσβασης (Physical Access Control).
  2. **Προσωρινή Αποθήκευση:** Τα δεδομένα παραμένουν τοπικά στην κονσόλα μόνο για το διάστημα της εξέτασης και διαγράφονται περιοδικά μετά την επιτυχή αρχειοθέτηση στο PACS (Data Purging Policy).

ΠΟΛΙΤΙΚΗ ΓΙΑ DATA-IN-TRANSIT ΑΣΦΑΛΕΙΑ

Έκδοση: 1.0

Ημερομηνία: Ιανουάριος 2026

1. Σκοπός

Διασφάλιση ότι όλα τα δεδομένα κατά τη μεταφορά είναι κρυπτογραφημένα και προστατευμένα από υποκλοπή (Man-in-the-Middle) ή μη εξουσιοδοτημένη πρόσβαση.

2. Τεχνολογίες Κρυπτογράφησης

- **TLS έκδοση:** 1.2 ή 1.3 (Απαγορεύονται SSL v3 / TLS 1.0/1.1).
- **VPN:**
    - **[X] IPSec** (Site-to-Site για σύνδεση με Κεντρικό Νοσοκομείο).
    - **[X] SSL VPN** (Για τον Vendor Support).
- **Εσωτερική κρυπτογράφηση υπηρεσιών:** Χρήση DICOM-TLS (Port 2762) για όλες τις εσωτερικές επικοινωνίες (π.χ. PACS προς Σταθμούς Εργασίας).

> **→ Εξαίρεση (Legacy Device):** Ο Μαγνητικός Τομογράφος (MRI Scanner), λόγω παλαιότητας λογισμικού (Legacy Asset), δεν υποστηρίζει κρυπτογράφηση TLS. Η επικοινωνία του παραμένει στη θύρα **DICOM 104 (Unencrypted)**.
>
> > **→ Αντισταθμιστικό Μέτρο:** Η κίνηση στη θύρα 104 περιορίζεται αυστηρά εντός του απομονωμένου **Medical VLAN (10.10.20.0/24)** και δεν δρομολογείται ποτέ εκτός αυτού, διασφαλίζοντας την προστασία από υποκλοπή στο ευρύτερο δίκτυο."

3. Σημεία Μεταφοράς Δεδομένων

- **Εσωτερικό δίκτυο:** Μεταφορά εικόνων από MRI Scanner σε Console και PACS.
- **Cloud:** Διασύνδεση με ΗΔΙΚΑ (MyHealth) και ΕΟΠΥΥ (HTTPS).
- **API/Integrations:** Ανταλλαγή δεδομένων HL7 με το Πληροφοριακό Σύστημα Νοσοκομείου (HIS).

4. Έλεγχος Ταυτότητας & Πρόσβασης

- **MFA για απομακρυσμένη πρόσβαση: [NAI]** (Υποχρεωτικό για Vendor & Administrators).
- **Certificate-based authentication: [NAI]** (Αμοιβαία πιστοποίηση - Mutual TLS για τη σύνδεση με το API της ΗΔΙΚΑ).

5. Παρακολούθηση

- **IDS/IPS:** Ενεργοποίηση στο Perimeter Firewall για εντοπισμό ύποπτης κίνησης στο DICOM πρωτόκολλο.

- **TLS inspection:** Εφαρμόζεται επιλεκτικά στην κίνηση προς Internet (Web Browsing ιατρών) για έλεγχο malware.

ΠΟΛΙΤΙΚΗ ΚΑΤΑΤΜΗΣΗΣ ΔΙΚΤΥΟΥ & ΑΣΦΑΛΟΥΣ ΠΡΟΣΒΑΣΗΣ ΕΦΟΔΙΑΣΤΙΚΗΣ ΑΛΥΣΙΔΑΣ

Έκδοση: 1.0

Ημερομηνία: Ιανουάριος 2026

1. Σκοπός

Ορισμός των μέτρων για δικτυακό διαχωρισμό και για ασφαλή διασύνδεση τρίτων (προμηθευτών, συνεργατών). Στόχος είναι η απομόνωση των κρίσιμων ιατρικών συστημάτων από το γενικό δίκτυο (Zero Trust) και η ελαχιστοποίηση του κινδύνου από επιθέσεις μέσω της εφοδιαστικής αλυσίδας (Supply Chain Attacks).

2. Κατάτμηση Δικτύου

- **Τμήματα του δικτύου (VLANs / Zones):**
    1. **Medical Zone (VLAN 20):** Υποδίκτυο **10.10.20.0/24**. Περιλαμβάνει MRI Scanner, Console, PACS Server.
    2. **Client Zone:** Σταθμοί εργασίας ιατρών και γραμματείας.
    3. **Management Zone:** Δικτυακός εξοπλισμός και διεπαφές διαχείρισης.
- **DMZ:** Δεν υφίσταται κλασική DMZ για δημόσια πρόσβαση, καθώς καμία υπηρεσία δεν εκτίθεται απευθείας στο Internet.
- **Κανόνες επικοινωνίας μεταξύ δικτυακών ζωνών:**
    1. Η επικοινωνία μεταξύ **Medical Zone** και **Hospital LAN** απαγορεύεται αυστηρά, εκτός από συγκεκριμένες πόρες (DICOM/HL7).
    2. Ο MRI Scanner **δεν έχει καμία** πρόσβαση στο Internet (Outbound Block).

3.Firewall & Access Rules

- **Firewall vendor:** Next-Generation Firewall (NGFW) με δυνατότητα Deep Packet Inspection (DPI) για ιατρικά πρωτόκολλα.
- **Policy set (Βάσει Task 1):**
    - **Inbound Rule:** Επιτρέπεται μόνο η κίνηση από τον HIS Server προς τον PACS Server (Ports 104, 2575) και η κίνηση VPN του Vendor. **Όλα τα άλλα: DENY.**
    - **Outbound Rule:** Επιτρέπεται η κίνηση HTTPS προς ΗΔΙΚΑ/ΕΟΠΥΥ μόνο από τα PC των Ιατρών. **MRI Scanner Outbound: DENY.**

- **Change control διαδικασία:** Κάθε αλλαγή στους κανόνες Firewall απαιτεί αίτημα αλλαγής (Change Request), αξιολόγηση ρίσκου και έγκριση από τον CISO (ΥΑΣΠΕ).

4. **Ασφαλής Πρόσβαση Προμηθευτών (Supply Chain Security)**
   - **Προμηθευτές που χρειάζονται πρόσβαση: MRI Vendor Support** (Συντήρηση/Troubleshooting).
   - **Τύποι πρόσβασης:**
     - **[X] VPN (Client-to-Site):** Ο τεχνικός συνδέεται με VPN Client και λαμβάνει IP από ειδικό Pool, χωρίς άμεση δρομολόγηση στο υπόλοιπο δίκτυο.
   - **Έλεγχοι ασφαλείας:**
     - **MFA (Multi-Factor Authentication): [NAI]** (Υποχρεωτικό για κάθε σύνδεση τρίτου).
     - **Περιορισμός ωραρίου πρόσβασης: [NAI]** (Η πρόσβαση ενεργοποιείται **μόνο κατόπιν αιτήματος** και για συγκεκριμένο χρονικό παράθυρο, π.χ. 2 ώρες).
     - **Monitor logs τρίτων:** Καταγραφή συνεδρίας (Session Recording) ή λεπτομερής καταγραφή (Audit Logs) για τις ενέργειες που εκτελεί ο προμηθευτής στα συστήματα.