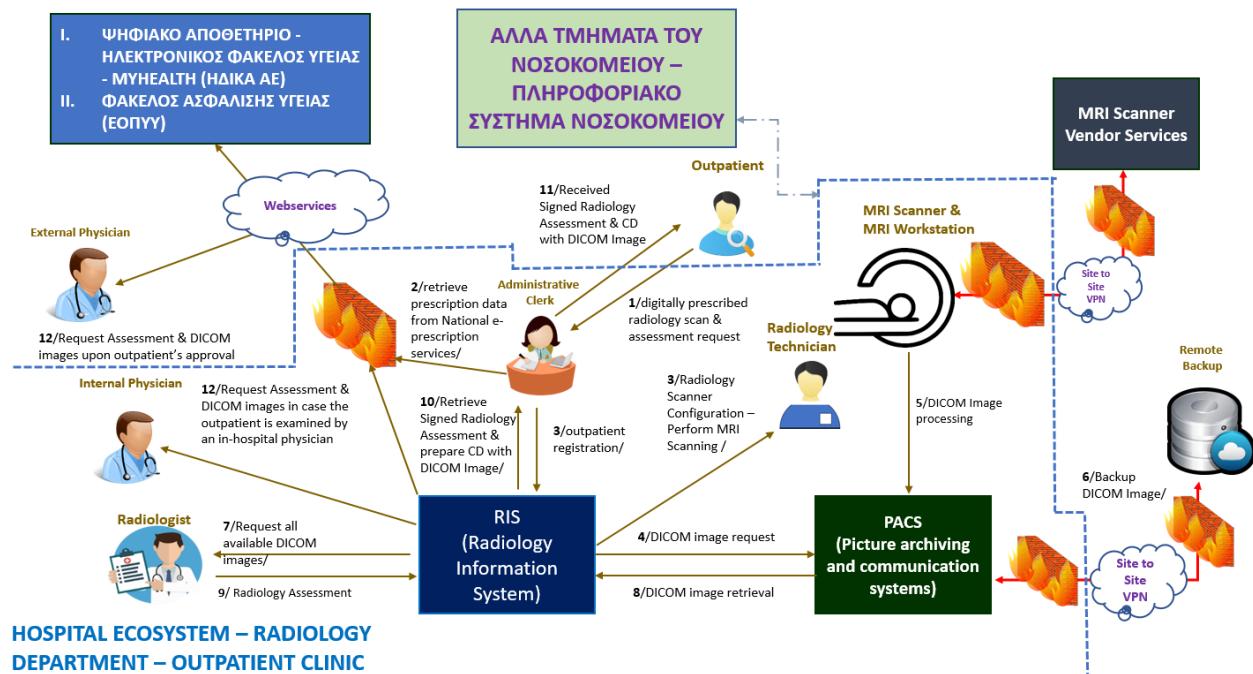


ΣΥΜΜΟΡΦΩΣΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΔΙΑΔΙΚΑΣΙΑΣ ΑΚΤΙΝΟΔΙΑΓΝΩΣΤΙΚΟΥ ΤΜΗΜΑΤΟΣ ΝΟΣΟΚΟΜΕΙΟΥ ΜΕ ΤΟΝ ΚΑΝΟΝΙΣΜΟ NIS 2

Σας δίδεται στο ακόλουθο σχήμα η επιχειρησιακή διαδικασία (ροή εργασιών) του Ακτινοδιαγνωστικού Τμήματος ενός Νοσοκομείου έχοντας οριστεί **Υπεύθυνος Ασφαλείας Συστημάτων Πληροφορικής και Επικοινωνιών** (ΥΑΣΠΕ).



Σε συνέχεια της προηγούμενης άσκησης να **Προτείνετε Πολιτικές Ασφαλείας και αντίστοιχα τεχνικά μέτρα για:**

- i. Πολιτική Ελέγχου Πρόσβασης και Ρόλων
- ii. Διαχείριση Ενημερώσεων των server, υπολογιστών κτλ. (Patch Management)
- iii. Διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων σε κατάσταση αδράνειας (data-at-rest)
- iv. Διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων κατά τη μεταφορά (data-in-transit)
- v. Καταρκεματισμό Δικτύου & ασφαλή πρόσβαση εφοδιαστικής αλυσίδας (εξωτερικές συνδέσεις)

Υπόδειξη: Συμπληρώστε τα παρακάτω template. Για την κατάρτιση των Πολιτικών Ασφαλείας μπορείτε να βασιστείτε στον οδηγό της <https://www.cisecurity.org-/media/project/cisecurity/cisecurity/data/media/files/uploads/2024/08/cis-ms-isac-nist-cybersecurity-framework-policy-template-guide-2024.pdf> και στην αντίστοιχη διάλεξη.

ΠΟΛΙΤΙΚΗ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ & ΡΟΛΩΝ (ACCESS CONTROL POLICY)

Έκδοση:

Ημερομηνία:

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 NIS2....**συμπληρώστε**

2. Πεδίο Εφαρμογής

Εφαρμόζεται σε

Χρήστες:

Συστήματα / Εφαρμογές:

Υποδομές / Δίκτυα:

3. Αρχές Ελέγχου Πρόσβασης

Ελάχιστο απαιτούμενο δικαιώμα (Least Privilege)

MFA για ευαίσθητα συστήματα: Ναι Όχι

Περιγράψτε.

4. Διαδικασία Δημιουργίας / Τροποποίησης / Απενεργοποίησης Λογαριασμών

Αίτηση πρόσβασης:

Έγκριση από:

Χρόνος απενεργοποίησης μετά από αποχώρηση:

Ετήσια αναθεώρηση ρόλων: Ναι / Όχι – Συχνότητα:

5. Έλεγχος Πρόσβασης σε Δεδομένα

Επίπεδα πρόσβασης:

Διαδικασία έγκρισης πρόσβασης σε ευαίσθητα δεδομένα:

6. Καταγραφή & Παρακολούθηση

Τι καταγράφεται (logs):

Χρόνος διατήρησης:

7. Εξαιρέσεις / Ειδικές Περιπτώσεις

Που δεν εφαρμόζεται;

ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΕΝΗΜΕΡΩΣΕΩΝ (PATCH MANAGEMENT)

Έκδοση:

Ημερομηνία:

1. Σκοπός

Η παρούσα πολιτική εξασφαλίζει ότι όλα τα συστήματα (servers, endpoints, δικτυακές συσκευές κ.λπ.) ενημερώνονται εγκαίρως για την αντιμετώπιση ευπαθειών. **Συμπληρώστε...**

2. Πεδίο Εφαρμογής

Servers:

Υπολογιστές:

Εξοπλισμός δικτύου:

3. Συχνότητα Ενημερώσεων

Κρίσιμες ενημερώσεις: εντός ωρών / ημερών

Ασφαλείας: Εβδομαδιαία Μηνιαία Άλλη:

Λειτουργικού συστήματος:

Εφαρμογών:

4. Διαδικασία Εντοπισμού Ευπαθειών

Εργαλεία που χρησιμοποιούνται:

Πηγή ενημερώσεων:

5. Διαδικασία Εφαρμογής

Έλεγχος συμβατότητας:

Δοκιμή σε περιβάλλον staging:

Εγκατάσταση:

Τεκμηρίωση:

Rollback plan:

Λεπτομέρειες:

6. Καταγραφή

Σημειώνονται όλα τα patches στο: Έγγρφο Excel Άλλο

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

Έκδοση:

Ημερομηνία:

1. Σκοπός

Προστασία δεδομένων που αποθηκεύονται σε servers, βάσεις δεδομένων, endpoints, φορητά μέσα και cloud. **Συμπληρώστε...**

2. Πεδίο Εφαρμογής

Συστήματα:

Βάσεις δεδομένων:

Αρχεία / Backups:

3. Εμπιστευτικότητα (Confidentiality)

Κρυπτογράφηση σε αποθήκευση (AES256/άλλο): Ναι / Όχι

Key management:

Πρόσβαση περιορισμένη σε χρήστες:...

4. Ακεραιότητα (Integrity)

Hashing / Checksum: Περιγράψτε τον αλγόριθμο

Logging αλλαγών αρχείων: Ναι / Όχι

Παρακολούθηση μη εξουσιοδοτημένων αλλαγών:

5. Διαθεσιμότητα (Availability)

Backups: Ημερήσιο Εβδομαδιαίο Άλλο:

Redundancy:....

RTO:

RPO:

ΠΟΛΙΤΙΚΗ ΓΙΑ DATA-IN-TRANSIT ΑΣΦΑΛΕΙΑ

Έκδοση:

Ημερομηνία:

1. Σκοπός

Διασφάλιση ότι όλα τα δεδομένα κατά τη μεταφορά είναι κρυπτογραφημένα και προστατευμένα από μη εξουσιοδοτημένη πρόσβαση. **Συμπληρώστε...**

2. Τεχνολογίες Κρυπτογράφησης

TLS έκδοση:

VPN: IPsec SSL VPN WireGuard Άλλο

Εσωτερική κρυπτογράφηση υπηρεσιών (service-to-service):

3. Σημεία Μεταφοράς Δεδομένων

Εσωτερικό δίκτυο:

Cloud:

API / Integrations:

4. Έλεγχος Ταυτότητας & Πρόσβασης

MFA για απομακρυσμένη πρόσβαση: Ναι Όχι

Certificate-based authentication: Ναι Όχι

5. Παρακολούθηση

IDS/IPS:

TLS inspection (αν εφαρμόζεται):

ΠΟΛΙΤΙΚΗ ΚΑΤΑΤΜΗΣΗΣ ΔΙΚΤΥΟΥ & ΑΣΦΑΛΟΥΣ ΠΡΟΣΒΑΣΗΣ ΕΦΟΔΙΑΣΤΙΚΗΣ ΑΛΥΣΙΔΑΣ

Έκδοση:

Ημερομηνία:

1. Σκοπός

Ορισμός των μέτρων για δικτυακό διαχωρισμό και για ασφαλή διασύνδεση τρίτων (προμηθευτών, συνεργατών). **Συμπληρώστε ...**

2. Κατάτμηση Δικτύου

Τμήματα του δικτύου (VLANs / Zones):

DMZ:

Κανόνες επικοινωνίας μεταξύ δικτυακών ζωνών:

3. Firewall & Access Rules

Firewall vendor:

Policy set:

Change control διαδικασία:

4. Ασφαλής Πρόσβαση Προμηθευτών

Προμηθευτές που χρειάζονται πρόσβαση:

Τύποι πρόσβασης (VPN, API, Portal):

Έλεγχοι ασφαλείας:

MFA: Ναι / Όχι

Περιορισμός ωραρίου πρόσβασης: Ναι / Όχι

Monitor logs τρίτων:

Το Παραδοτέο της άσκησης είναι 1 Αρχείο (pdf ή word) με τις Πολιτικές Ασφαλείας και των αντίστοιχων τεχνικών μέτρων που πρέπει να εφαρμοστούν