Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά Συστήματα

Μελέτη Ασφάλειας Πληροφοριακού Συστήματος Δημόσιου Νοσοκομείου

Ναπολέων Λύγδας

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Μάιος 2013

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μελέτη Ασφάλειας Πληροφοριακού Συστήματος Δημόσιου Νοσοκομείου

Ναπολέων Λύγδας

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2013

Περίληψη

Στη παρούσα μεταπτυχιακή διατριβή θα εκπονηθεί η μελέτη ασφάλειας ενός πληροφοριακού συστήματος ενός υποθετικού δημόσιου Νοσοκομείου.

Τα δεδομένα τα οποία διαχειρίζεται το πληροφοριακό σύστημα ενός νοσοκομείου είναι κυρίως ευαίσθητα προσωπικά δεδομένα και δεδομένα που υπόκεινται στο Ιατρικό Απόρρητο. Είναι λοιπόν απαραίτητο να υπάρχει ασφάλεια υψηλού βαθμού σε αυτό, για την προστασία της Εμπιστευτικότητας των δεδομένων αυτών.

Επίσης θα πρέπει να προστατευτούν η Ακεραιότητα και η Διαθεσιμότητα των δεδομένων του νοσοκομείου, αφού από αυτά εξαρτάται η απρόσκοπτη και αποτελεσματική παροχή των υπηρεσιών υγείας στους πολίτες.

Στη μεταπτυχιακή διατριβή θα γίνει μια γενική περιγραφή των υπηρεσιών υγείας στην Ελλάδα και η περιγραφή του πληροφοριακού συστήματος του υποθετικού νοσοκομείου.

Θα παρουσιαστούν το πρότυπα και η μεθοδολογία που θα χρησιμοποιηθούν στη μελέτη ασφάλειας και συγκεκριμένα το πρότυπο ISO/IEC 27001:2005 και η μέθοδος OCTAVE Allegro.

Σύμφωνα με αυτά θα γίνει Εκτίμηση του Κινδύνου για τα Αγαθά του πληροφοριακού συστήματος και θα εκπονηθεί το Σχέδιο Ασφάλειας του νοσοκομείου και το Σχέδιο Ανάκαμψης από Καταστροφή. Το Σχέδιο Ασφάλειας περιλαμβάνει την Πολιτική Ασφάλειας και τα απαιτούμενα μέτρα για την προστασία των Αγαθών του πληροφοριακού Συστήματος.

Το Σχέδιο Ανάκαμψης από Καταστροφή περιλαμβάνει τις απαραίτητες ενέργειες για την επαναφορά του συστήματος σε λειτουργία μετά από μια καταστροφή.

Επίσης θα εκπονηθεί Κώδικας Δεοντολογίας, για το προσωπικό του νοσοκομείου που δεν δεσμεύεται από το Ιατρικό Απόρρητο, ο οποίος θα περιλαμβάνει τις διαδικασίες που πρέπει να ακολουθεί το προσωπικό για την προστασία της Εμπιστευτικότητας των Ιατρικών δεδομένων.

Summary

In this master thesis, the security of an information system of a hypothetical public hospital, will be studied.

The data managed by the information system of a hospital are mostly sensitive personal data and data subject to Medical Confidentiality. It is important to have a high degree of safety in this to protect the Confidentiality of such data.

Moreover, Integrity and Availability of data must be protected, since from them depends the smooth and efficient delivery of health services to the citizens.

In the thesis it will be given a general description of health services in Greece and the description of the information system of the hypothetical hospital.

The standards and methodologies that will be used in safety study will be presented, specifically the standard ISO / IEC 27001:2005 and the method OCTAVE Allegro.

According to them, a Risk Assessment for the Assets of the information system will be undertaken and Safety Plan and Disaster Recovery Plan of the hospital will be prepared. Security Plan includes Security Policy and Measures that are required to protect the Assets of the information system.

The Disaster Recovery Plan includes the necessary procedures to restore the system's operation after a disaster.

A Code of Ethics for the hospital staff non - aligned by medical confidentiality, will be also carried, with the procedures that staff has to follow to protect the confidentiality of medical data.

Ευχαριστίες

Ευχαριστώ τον επιβλέποντα καθηγητή μου κ. Στέφανο Γκρίτζαλη για την υποστήριξή του στην εκπόνηση της παρούσας μεταπτυχιακής διατριβής.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Περιγραφή των δομών της Υγείας στην Ελλάδα και των προσπαθειών που γίνονται για την βελτίωση των παρεχόμενων υπηρεσιών στους πολίτες.

1.1 Η Υγεία στην Ελλάδα

Στο Εθνικό Σχέδιο Δράσης για την Υγεία 2008 – 2012, αναφέρεται ότι:

"Είναι γενικά παραδεκτό, ότι η υγεία και η παιδεία συνιστούν τη θεμελιώδη προϋπόθεση για τη διατήρηση και τη βελτίωση του ανθρώπινου και διανοητικού κεφαλαίου στις σύγχρονες κοινωνίες και, κατά συνέπεια, προσδιορίζονται ως υψηλή κοινωνική προτεραιότητα. Η Δημόσια Υγεία αποτελεί ένα κοινωνικό, πολιτικό και διοικητικό εγχείρημα διαχείρισης και ελέγχου των μειζόνων παραγόντων κινδύνου για την υγεία και βελτίωσης του επιπέδου υγείας του πληθυσμού…[22]."

Θεωρώντας την υγεία των πολιτών θεμελιώδες κεφάλαιο για την κοινωνία, γίνονται προσπάθειες για την αναβάθμιση του Εθνικού Συστήματος Υγείας (ΕΣΥ). Μέσω του Ν. 3329/2005 δημιουργήθηκαν δεκαεπτά διοικητικές Υγειονομικές Περιφέρειες – Υ.ΠΕ. Σε κάθε Υ.ΠΕ. ανήκουν διοικητικά ένας αριθμός νοσοκομείων και δομές πρωτοβάθμιας φροντίδας. Οι Υ.ΠΕ. συγχωνεύθηκαν σε επτά με το Ν. 3527/2007 και είναι οι ακόλουθες:

1η Υ.ΠΕ. Αττικής

2η Υ.ΠΕ. Πειραιώς και Αιγαίου

3η Υ.ΠΕ. Μακεδονίας

4η Υ.ΠΕ. Μακεδονίας και Θράκης

5η Υ.ΠΕ. Θεσσαλίας και Στερεάς Ελλάδας

6η Υ.ΠΕ. Πελοποννήσου, Ιονίων Νήσων, Ηπείρου και Δ. Ελλάδας

7η Υ.ΠΕ. Κρήτης

Έτσι όσον αφορά τη δομή της Δημόσιας Υγείας έχουμε τέσσερα επίπεδα, η διαβάθμιση των οποίων είναι η εξής:

4ο επίπεδο: Υπουργείο Υγείας και Κοινωνικής Αλληλεγγύης – ΥΥΚΑ

3ο επίπεδο: Υγειονομικές Περιφέρειες - Υ.ΠΕ.

2ο επίπεδο: Νοσοκομείο

1ο επίπεδο: Πρωτοβάθμια φροντίδα (Κέντρα Υγείας - ΚΥ και τα Περιφερειακά Ιατρεία - ΠΙ)

Οι αναγκαίες μεταρρυθμίσεις που πρέπει να εφαρμοστούν, ορίζονται στους παρακάτω 10 άξονες της Νέας Εθνικής Στρατηγικής για την Υγεία.

1. Οικονομική εξυγίανση του ΕΣΥ και εξασφάλισης της βιωσιμότητάς του.
2. Θεμελίωση σύγχρονου δικτύου Πρωτοβάθμιας Φροντίδας.
3. Δυναμική προώθηση της προληπτικής πολιτικής.
4. Εισαγωγή της πληροφορικής και των νέων τεχνολογιών σε όλα τα επίπεδα της δημόσιας διοίκησης.

5. Νέα πολιτική για το ανθρώπινο δυναμικό.
6. Μεταρρύθμιση της Ψυχικής και Δημόσιας υγείας.
7. Ανάπτυξη και προαγωγή του εθελοντισμού και της κοινωνικής εταιρικής ευθύνης.
8. Προώθηση της εκπαίδευσης, έρευνας και καινοτομίας.
9. Πολιτική συμπράξεων με τον ιδιωτικό τομέα.
10. Προώθηση της Ελλάδας στην Παγκόσμια Αγορά και Κοινωνία της Υγείας.

Είναι πια κοινός τόπος ότι οι Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ), αποτελούν ακρογωνιαίο λίθο στον εκσυγχρονισμό και βελτίωση της Δημόσιας Υγείας. Έτσι ο 4ος άξονας της Νέας Εθνικής Στρατηγικής για την Υγεία ανάμεσα στα άλλα θέτει σαν προτεραιότητα την Ολοκλήρωση των Πληροφοριακών Συστημάτων στα νοσοκομεία. Το 2002 στο Επιχειρησιακό Σχέδιο του ΥΥΚΑ για την «Κοινωνία της Πληροφορίας» αναφέρονταν τα εξής:

«...είναι φανερό ότι θα πρέπει να αναζητηθούν οι διαδικασίες εκείνες που θα επιτρέψουν ένα ελάχιστο (κατά περίπτωση) απαιτούμενο επίπεδο πληροφοριακής οργάνωσης, προκειμένου να βελτιωθεί αισθητά ο παραδοσιακός τρόπος λειτουργίας των Νοσοκομείων και να διευκολυνθεί η Κεντρική Υπηρεσία της Υγειονομικής Περιφέρειας - ΥΠΕ (τέως ΔΥΠΕ, τέως ΠεΣΥΠ) στη συλλογή και συστηματική παρακολούθηση στοιχείων για τη λήψη αποφάσεων που αφορούν το χώρο της Υγείας. Για το λόγο αυτό έχουν προδιαγραφεί τα ακόλουθα επίπεδα πληροφοριακής οργάνωσης στα οποία μπορεί να φτάσει ένα Νοσοκομείο.

Επίπεδο 1	Βασικός πυρήνας διαχειριστικών εφαρμογών (πχ. Γραφείο Κίνησης, Εξωτερικά Ιατρεία, Φαρμακείο – ατομικό συνταγολόγιο, Νοσήλια, Λογιστήριο – διπλογραφικό, Διαχείριση Υλικών κλπ.).
Επίπεδο 2	Εργαστηριακά συστήματα σε βασικά νοσοκομειακά εργαστήρια (πχ. Βιοχημικό, μικροβιολογικό, αιματολογικό)
Επίπεδο 3	Σύστημα έκδοσης εντολών προς εργαστήρια, φαρμακείο, νοσήλια στις κλινικές κλπ.
Επίπεδο 4	Τεχνολογία bar code σε φάρμακα, εξετάσεις, αντιδραστήρια κλπ.
Επίπεδο 5	Εντολές ιατρικής/νοσηλευτικής φροντίδας, ιστορικό ασθενούς

Επίπεδο 6	Επεξεργασία ιατρικής εικόνας (πχ. οργάνωση ακτινολογικών εργαστηρίων, παροχή υπηρεσιών τηλεδιάγνωσης μέσω εικόνας κλπ.)
Επίπεδο 7	Πρωτόκολλα κατευθυνόμενης περίθαλψης, υποστήριξη στην λήψη αποφάσεων

Πίνακας 1.1: Επίπεδα πληροφοριακής οργάνωσης Δημόσιου Νοσοκομείου

Ανεξάρτητα από τη διαβάθμιση που θα αποφασιστεί ανά νοσοκομείο και ΠεΣΥ, για να επιτευχθούν οι στόχοι που έχουν τεθεί για τη πληροφοριακή οργάνωση των Υγειονομικών Περιφερειών (πρώην ΔΥΠΕ, πρώην ΠΕΣΥΠ), θα πρέπει όλα τα νοσοκομεία της χώρας να φτάσουν τουλάχιστο στο 3ο επίπεδο όσον αφορά την πληροφοριακή τους υποδομή.»

Για την επίτευξη του παραπάνω στόχου αναπτύχθηκαν στις Υ.ΠΕ. και στα νοσοκομεία που τις απαρτίζουν, με πόρους από το Επιχειρησιακό Πρόγραμμα Κοινωνία της Πληροφορίας (ΚτΠ), **Ολοκληρωμένα Πληροφοριακά Συστήματα Υγείας (ΟΠΣΥ).**

Το ΟΠΣΥ είναι ένα κατανεμημένο σύστημα (distribute system) που περιλαμβάνει μια συλλογή ανεξάρτητων πληροφοριακών συστημάτων καθένα από τα οποία εξυπηρετεί τις διαφορετικές μονάδες της Υ.Πε. Περιλαμβάνει το ολοκληρωμένο **Πληροφοριακό Σύστημα του Νοσοκομείου** (Hospital Information System - HIS) και τα **Πληροφοριακά Συστήματα των Κ.Υ**. Επίσης περιλαμβάνει ένα σύστημα διασύνδεσης των νοσοκομείων, των Κ.Υ. και της διοίκησης της Υ.Πε.

Για την απόλυτη κατανόηση του όρου Πληροφοριακό Σύστημα δίνονται οι παρακάτω ορισμοί, οι οποίοι τον καθορίζουν με σαφήνεια και πληρότητα στα διαδοχικά τους βήματα.

Πληροφοριακό Σύστημα Υγείας – ΠΣΥ (Healthcare Information System - HIS) είναι το πληροφοριακό σύστημα στον τομέα της Υγείας. [02]

Ειδικότερα, **Πληροφοριακό Σύστημα (Information System)** είναι [03] ένα Υπολογιστικό Συγκρότημα μαζί με τις πληροφορίες που διαχειρίζεται, όπου:

Υπολογιστικό Συγκρότημα (IT Assembly) είναι μια συλλογή υπολογιστικού υλικού, λογισμικού, τηλεπικοινωνιακού εξοπλισμού ή άλλων υπολογιστικών εξαρτημάτων που χρησιμοποιούνται για τη διαχείριση πληροφοριών.

Πληροφορία (information) είναι τα δεδομένα μαζί με την έννοια που τους αποδίδεται.

Δεδομένα (data) είναι ένα σύνολο κατανοητών συμβόλων που έχουν καταγραφεί.

Υπολογιστικός Πόρος (IT Resource) είναι οτιδήποτε αξιοποιείται από ένα υπολογιστικό σύστημα για να διαχειριστεί πληροφορίες.

Εφαρμογή (Application) είναι οι πληροφορίες, λογισμικό και διαδικασίες που έχουν σχεδιαστεί για την επίτευξη συγκεκριμένων στόχων (Δηλαδή ένας συνδυασμός Υπολογιστικών πόρων και Πληροφοριών).

Στο πλαίσιο της προσπάθειας διείσδυσης των ΤΠΕ στον τομέα Δημόσιας Υγείας και της αναβάθμισης της ποιότητας των παρεχόμενων υπηρεσιών στους πολίτες, δημιουργήθηκαν από την Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλισης Α.Ε. – ΗΔΙΚΑ δύο εφαρμογές. Η εταιρεία ΗΔΙΚΑ είναι δημόσια επιχείρηση η οποία εποπτεύεται από το ΥΥΚΑ και δημιούργησε την εφαρμογή ηλεκτρονικής συνταγογράφησης (e-syntagografisi) και την εφαρμογή ηλεκτρονικής παραγγελίας εξετάσεων (e-diagnosis). Στις 14/1/2012 τέθηκε σε παραγωγική λειτουργία μια νέα εφαρμογή η οποία αποτελεί την ενοποίηση των δύο παραπάνω. Με αυτό τον τρόπο δίνεται η δυνατότητα της καταχώρησης συνταγών και παραπεμπτικών μέσα από ένα σύστημα, απλουστεύοντας τη διαδικασία συνταγογράφησης για τους χρήστες ιατρούς και μειώνοντας το χρόνο έκδοσης, εκτέλεσης συνταγής και παραπεμπτικού [04]. Η καταχώρηση μέσω της εφαρμογής είναι υποχρεωτική.

Η τηλεπικοινωνιακή διασύνδεση των νοσοκομείων υλοποιείται με το έργο «ΣΥΖΕΥΞΙΣ». Το «ΣΥΖΕΥΞΙΣ» είναι ένα έργο του Υπουργείου Διοικητικής Μεταρρύθμισης & Ηλεκτρονικής Διακυβέρνησης (ΥΔΜΗΔ), με το οποίο επιδιώκεται η ανάπτυξη και ο εκσυγχρονισμός της τηλεπικοινωνιακής υποδομής του Δημόσιου Τομέα. Πρόκειται για ένα δίκτυο πρόσβασης και κορμού για τους φορείς του Δημοσίου, με σκοπό να καλύψει όλες τις ανάγκες για τη μεταξύ τους επικοινωνία με **Τηλεφωνία** (τηλεφωνική επικοινωνία ανάμεσα στους φορείς), **Δεδομένα** (επικοινωνία υπολογιστών - Internet) και **Video** (τηλεδιάσκεψη – τηλεεκπαίδευση). Σκοπός του έργου είναι **η βελτίωση της λειτουργίας των δημοσίων υπηρεσιών**, με την αναβάθμιση της μεταξύ τους επικοινωνίας μέσω της παροχής προηγμένων τηλεματικών υπηρεσιών με χαμηλό κόστος, και **η ενοποιημένη εξυπηρέτηση των πολιτών**, με αυτοματοποιημένα και φιλικά προς τον χρήστη συστήματα πληροφόρησης και διεκπεραίωσης συναλλαγών με το Δημόσιο [05].

1.2 Ηλεκτρονικός Φάκελος Ασθενή

Βασική δομή του ΟΠΣΥ είναι ο **Ηλεκτρονικός Φάκελος Ασθενή (ΗΦΑ) ή Ηλεκτρονικός Φάκελος Υγείας (ΗΦΥ) ή Ηλεκτρονικός Ιατρικός Φάκελος (ΗΙΦ)**. Ο ΗΦΑ είναι μια διαχρονική ηλεκτρονική καταγραφή των πληροφοριών για την υγεία ενός ασθενή, οι οποίες παράγονται σε μια ή περισσότερες επαφές του ασθενή με ειδικούς υγείας. Αυτές οι πληροφορίες περιλαμβάνουν δημογραφικά στοιχεία του ασθενή, προβλήματα, φαρμακευτική αγωγή, καταγραφή εξέλιξης του ασθενή, ζωτικές παραμέτρους, ιατρικό ιστορικό, εμβολιασμούς, εργαστηριακά δεδομένα και ακτινοδιαγνωστικές αναφορές. Ο ΗΦΑ αυτοματοποιεί, εκσυγχρονίζει, απλοποιεί την ροή εργασίας του κλινικού γιατρού και παρέχει ένα πλήρες αρχείο των κλινικών επαφών του ασθενή. Επίσης υποστηρίζει άμεσα ή έμμεσα τις δραστηριότητες για την παροχή φροντίδας, όπως υποστήριξη αποφάσεων, διαχείριση ποιότητας και την αναφορά αποτελεσμάτων [06].

Οι οδηγίες του Υπουργείου Υγείας για τον ΗΦΑ ορίζουν τα παρακάτω υποσυστήματα που τον αποτελούν, τις προδιαγραφές που πρέπει να ικανοποιεί και τα παραγόμενα έντυπα [07]:

1.2.1 Υποσυστήματα στο ΟΠΣΥ για το Φάκελο Ασθενή

1. **Διαχειριστικό τμήμα που περιλαμβάνει:**
    1.1. Διαχείριση επισκέψεων – Ραντεβού (ΤΕΙ)
    1.2. Επείγοντα Περιστατικά (ΤΕΠ)
    1.3. Κλινικές/Μονάδες/Χειρουργείο
    1.4. Ιατρική Απεικόνιση (διασυνδεόμενο με το Radiology Information System - RIS)
    1.5. Βιοπαθολογικά Εργαστήρια (διασυνδεόμενο με το Laboratory Information System)
    1.6. Φαρμακευτικό και Υγειονομικό Υλικό
    1.7. Διοίκηση (administration & overheads)
    1.8. Οικονομικό τμήμα (ΚΕΝ)
2. **<u>Ιατρικό – Νοσηλευτικό Υποσύστημα Φακέλου Ασθενή</u>**

2.1. **Εξωτερικά Ιατρεία – Επείγοντα Περιστατικά** (Κοινό Υποσύνολο με το Υποσύστημα Διαχείρισης Ασθενών).

2.1.1. Διαχείριση και παρακολούθηση των ασθενών που επισκέπτονται τα ΤΕΙ ή τα ΤΕΠ (Επισκέψεις/Εξετάσεις ασθενών, φάκελος ασθενή, εισαγωγή εξωτερικού ασθενή) των Νοσοκομείων ή των Μονάδων Πρωτοβάθμιας Φροντίδας Υγείας (ΠΦΥ).

2.1.2. Διασύνδεση με το υποσύστημα της γραμματείας εξωτερικών ιατρείων ώστε να παρακολουθούνται πλήρως οι προγραμματισμένες επισκέψεις ασθενών.

2.1.3. Διαχείριση των εντολών τακτικής/έκτακτης εισαγωγής ασθενούς και της ενημέρωσης του γραφείου εισαγωγών και κίνησης.

2.2. **Ιατρικές Πράξεις – Φάρμακα/Υλικό – Ηλεκτρονικές Παραγγελίες (Order Entry) – Παραπεμπτικά** (Κοινό Υποσύνολο με το Υποσύστημα Διαχείρισης Ασθενών).

2.2.1. Οργάνωση και προγραμματισμός των ανθρωπίνων και υλικών πόρων του νοσοκομείου για την εκτέλεση ιατρικών εντολών, την αυτόματη παραγγελία ιατρικών πράξεων και εξετάσεων (ηλεκτρονικά παραπεμπτικά, παραγγελία κλινικών/παρακλινικών εξετάσεων, χειρουργικές επεμβάσεις κτλ) και την παραλαβή και επισκόπηση των αποτελεσμάτων και πορισμάτων ηλεκτρονικά.

2.2.2. Δυνατότητα online παραγγελίας και έκδοσης παραπεμπτικών κάθε μορφής (εργαστηριακές, ακτινολογικές εξετάσεις, χορηγήσεις φαρμάκων, οδηγίες νοσηλευτών).

2.3. **Ιατρικά Πρωτόκολλα – Ιατρικά Πορίσματα**

2.3.1. Δημιουργία ηλεκτρονικών εγγράφων με τη χρήση προτυποποιημένων εντύπων για την καταγραφή των ιατρικών, θεραπευτικών και νοσηλευτικών δεδομένων που συμπληρώνονται από το ιατρικό και νοσηλευτικό προσωπικό και αφορούν την τεκμηρίωση των διαγνώσεων, των θεραπευτικών αγωγών και άλλων ιατρικών δεδομένων κατά την εισαγωγή, παραμονή, θεραπεία και έξοδο του ασθενή.

2.4. Ιατρικό Ιστορικό – Διαγνώσεις

2.4.1. Καταγραφή των διαγνώσεων (εισόδου - εξόδου), του ιατρικού ιστορικού και γενικότερα της ιατρικής κατάστασης του ασθενούς.

2.5. Νοσηλευτική Υπηρεσία

2.5.1. Οργάνωση της νοσηλευτικής υπηρεσίας του νοσοκομείου για την παροχή νοσηλευτικής φροντίδας, τη χορήγηση φαρμάκων, την τήρηση της θεραπευτικής αγωγής του ασθενούς και γενικότερα την παρακολούθηση της πορείας της νόσου, σε άμεση συνεργασία με την εφαρμογή των ιατρικών πράξεων, για την ενημέρωση και παροχή πληροφόρησης του νοσηλευτικού προσωπικού σχετικά με τη θεραπευτική αγωγή που πρέπει να ακολουθήσει ο ασθενής.

1.2.2 Έντυπα του ΟΠΣΥ

Τα έντυπα που απαιτούνται στο ΟΠΣΥ είναι τα εξής:

Φ1 701β – Ατομική Συνταγή Φαρμάκων και Χρεωμένου Υγειονομικού Υλικού .

Ε1 602 – Παραπεμπτικό Αιματολογικών Εξετάσεων .

Ε1 603 – Παραπεμπτικό Βιοχημικών Εξετάσεων .

Ε1 604 – Παραπεμπτικό Μικροβιολογικών Εξετάσεων .

Ε1 607 Παραπεμπτικό Εργαστηριακών Εξετάσεων Μεταδιδόμενων με το Αίμα Νοσημάτων.

Ε2 612 – Παραπεμπτικό Ακτινολογικών Εξετάσεων .

Ε2 614 – Παραπεμπτικό Ειδικού Απεικονιστικού Ελέγχου.

Ε2 615 – Παραπεμπτικό υπερηχογραφήματος – Tripplex .

Ν1 501 – Νοσηλευτικό Ιστορικό.

Ν1 521 – Ημερήσιο Φύλλο Νοσηλείας .

Ν2 531 – Δελτίο Παραγγελίας Αναλωσίμου Υγειονομικού Υλικού .

Ν2 532 – Γενικό Συνταγολόγιο Παραγγελίας Νοσηλευτικού Υλικού Φαρμακείου.

Ι1 401 – Φύλλο Ιστορικού Ασθενή.

I1 421 – Καρτέλα Τακτικών Εξωτερικών Ιατρείων .

I1 422 – Φύλλο Ασθενούς ΤΕΠ .

I1 423 – Φύλλο Βραχείας Νοσηλείας.

I4 471 – Ενημερωτικό Σημείωμα.

I4 472 – Ιατρική Βεβαίωση - Γνωμάτευση .

1.2.3 Πρότυπα και Κωδικοποιήσεις

Σε ένα πληροφοριακό σύστημα υγείας τα δεδομένα που επεξεργάζονται και η παραγόμενη πληροφορία είναι πολλών τύπων (π.χ. ακτινογραφίες, καρδιογραφήματα, υπέρηχοι, πληροφορία σε κάποιο επεξεργαστή κειμένου κλπ). Για την επικοινωνία των διαφορετικών κατανεμημένων συστημάτων μεταξύ τους είναι απαραίτητη η δυνατότητα διασυνδεσιμότητας και ενοποίησης της πληροφορίας. Στο πλαίσιο αυτό έχουν δημιουργηθεί διεθνώς αποδεκτές τυποποιήσεις (πρωτόκολλα). Μερικά από αυτά είναι:

1. Το αμερικανικό πρότυπο **HL7**, το οποίο αναπτύχθηκε από τον μη κερδοσκοπικό οργανισμό Health Level 7. Το HL7 αποτελεί μια προσέγγιση ολοκλήρωσης των συστημάτων η οποία είναι δοκιμασμένη και επιτυγχάνει στο επίπεδο της ολοκλήρωσης των δεδομένων. Ένας μεγάλος αριθμός κατασκευαστών ιατροτεχνολογικών προϊόντων και μικροβιολογικού υλικού ανέπτυξε μηχανήματα συμβατά με το πρότυπο αυτό για να διευκολυνθεί η ροή της πληροφορίας και η επικοινωνία με τα άλλα συστήματα του νοσοκομείου.

2. Το ευρωπαϊκό πρότυπο **ENV 1306** του Ευρωπαϊκού Οργανισμού Τυποποίησης (CEN-TC 251), που ορίζει την αρχιτεκτονική των ιατρικών φακέλων.

3. Το πρότυπο **Digital Imaging and Communications in Medicine – DICOM** από τον αμερικανικό οργανισμό American College of Radiology – National Electrical Manufacture's Association (ACR-NEMA), για διαγνωστικές απεικονιστικές εξετάσεις.

4. Το ευρωπαϊκό πρότυπο **SCP-ECG** του Ευρωπαϊκού Οργανισμού Τυποποίησης (CEN-TC 251), το οποίο υποστηρίζει σε αντιστοιχία με το DICOM την κωδικοποίηση και μεταφορά ηλεκτροκαρδιογραφήματος.

5. Το **Picture Archiving and Communication System – PACS** το οποίο συλλέγει, επεξεργάζεται, διανέμει, αποθηκεύει, αρχειοθετεί και απεικονίζει ιατρικές εικόνες.

6. Το **Rhapsody Integration Engine** της αμερικανικής εταιρείας Orion Health είναι ένα ενδιάμεσο ισχυρό πληροφοριακό σύστημα (middleware) το οποίο επιτρέπει την διασύνδεση μεταξύ πολλαπλών διαφορετικών πληροφοριακών συστημάτων. Παρέχει στους Φορείς Υγείας (και όχι μόνο) την δυνατότητα να επικοινωνούν μεταξύ τους αλλά και να διασυνδέουν τα πληροφοριακά συστήματά τους προσφέροντας ολοκληρωμένη και ενοποιημένη πληροφόρηση στους χρήστες. Το Rhapsody Integration Engine παρέχει στους φορείς υγείας μια ολοκληρωμένη λύση πακέτο στο παραπάνω πρόβλημα παρέχοντας την δυνατότητα εύκολης και ασφαλούς διασύνδεσης των πληροφοριακών τους συστημάτων. Το Rhapsody προσφέρει ανεπτυγμένες δυνατότητες messaging στους υγειονομικούς και νοσοκομειακούς οργανισμούς όλων των μεγεθών. Διασφαλίζει αυτόματες επικοινωνίες μεταξύ των IT συστημάτων, ανεξάρτητα από κάθε format και πρωτόκολλο [09]. Μερικά από τα πλεονεκτήματα που προσφέρει η χρήση του στους οργανισμούς και στους χρήστες στον τομέα της υγείας είναι τα ακόλουθα:

   - ενοποιεί, ολοκληρώνει, αυτοματοποιεί και ομαλοποιεί τις επιχειρησιακές διαδικασίες και την ανταλλαγή δεδομένων ανάμεσα σε πολλαπλά, ανόμοια συστήματα,
   - επιτρέπει την αλάνθαστη ανταλλαγή μηνυμάτων με οργανισμούς και συστήματα εκτός οργανωμένων μονάδων,
   - απλοποιεί τη δημιουργία και διαχείριση των εφαρμογών διασύνδεσης μεταξύ ήδη εγκατεστημένων συστημάτων εφαρμογών,
   - ελαχιστοποιεί το ρίσκο για λάθος που σχετίζεται με χειροκίνητες διαδικασίες μετάδοσης του μηνύματος.

7. **Διεθνές Πρότυπο Ταξινόμησης Ασθενειών (International Classification of Diseases - ICD-10)**. Επειδή είναι αναγκαία η ύπαρξη μιας κοινής γλώσσας ιατρικής ορολογίας για την επίλυση ασαφειών στην ανταλλαγή δεδομένων ασθενών ανάμεσα σε ειδικούς υγείας δημιουργήθηκαν συστήματα ταξινόμησης και κωδικοποίησης της πληροφορίας υγείας. Σκοπός τους είναι να βελτιστοποιηθεί η συλλογή και επεξεργασία της ηλεκτρονικής αυτής πληροφορίας σε ότι αφορά νόσους, διαγνώσεις και η συλλογή και επεξεργασία της ηλεκτρονικής αυτής πληροφορίας που είναι απαραίτητη στη λήψη ιατρονοσηλευτικών αποφάσεων καθώς και στις επιδημιολογικές, υγειονομικές και κλινικοεργαστηριακές

αποφάσεις [02]. Σημαντική κωδικοποίηση για αυτό το σκοπό είναι το διεθνές πρότυπο ταξινόμησης ασθενειών **ICD-10**.

8. **Παγκόσμια Ταξινόμηση Πρωτοβάθμιας Φροντίδας, 2η έκδοση (International Classification of Primary Care – ICPC, 2R)**. Η κωδικοποίηση αυτή είναι κατάλληλη για την Γενική/Οικογενειακή Ιατρική και την Πρωτοβάθμια Φροντίδα.

9. **Anatomic Therapeutical Classification System – ATC**, που είναι κωδικοποίηση των φαρμάκων.

10. **Κωδικοποίηση Φαρμάκων του Εθνικού Οργανισμού Φαρμάκων – ΕΟΦ.**

11. **Ελληνική Ονοματολογία και Κωδικοποίηση των Ιατρικών Πράξεων (ΕΛ.Ο.Κ.Ι.Π.)** η οποία καθορίστηκε από το Κεντρικό Συμβούλιο Υγείας (ΚΕ.Σ.Υ.). Η ΕΛ.Ο.Κ.Ι.Π. σύμφωνα με την με αρ. πρωτ. Υ4α/οικ.25184/ 13-03-2012 εγκύκλιο του ΥΥΚΑ «είναι απαραίτητη σε κάθε ιατρική διαδικασία καθώς διευκολύνει τις διοικητικές και οικονομικές διαδικασίες των υπηρεσιών υγείας, περιορίζει τα λάθη και έχει εφαρμογή στα πληροφοριακά συστήματα των Νοσοκομείων» [10].

12. **Κλειστά Ενοποιημένα Νοσήλια – ΚΕΝ (**Diagnosis related group – DRGs). Από την 1/10/11 το Υπουργείο Υγείας και Κοινωνικής Αλληλεγγύης έχει ορίσει ότι η τιμολόγηση των ασθενών θα γίνεται με βάση τα **ΚΕΝ**. Σε αυτό το σύστημα "… ο κάθε ασθενής κατατάσσεται με βάση τη διάγνωση, τα χαρακτηριστικά του και τις υπηρεσίες που του παρέχονται σε μια συγκεκριμένη κατηγορία, στην οποία έχει προκαθοριστεί μια συγκεκριμένη αμοιβή που καθορίζεται με βάση τεκμηριωμένα, αποτελεσματικά και αποδοτικά πρότυπα παροχής φροντίδας και καταβάλλεται από τον πληρωτή ανεξάρτητα από το πραγματικό τελικό κόστος του ασθενούς για τον παραγωγό. Το σύστημα αυτό εξαναγκάζει τα νοσοκομεία να εφαρμόσουν τα αποδοτικά πρότυπα παροχής και να μειώσουν το λειτουργικό τους κόστος. Επίσης κάνει ευκολότερη τη μέτρηση του αποτελέσματος, τις συγκρίσεις μεταξύ δημόσιων και ιδιωτικών παραγωγών και τη σύνταξη προϋπολογισμών για τα νοσοκομεία και τους ασφαλιστικούς φορείς. Για να εφαρμοστεί ένα σύστημα με βάση τα DRGs απαιτούνται:

    - ένα σύστημα κωδικοποίησης και ταξινόμησης των ασθενών με βάση τη διάγνωση, που καθολικά σχεδόν είναι το ICD-10

- ένα σύστημα κωδικοποίησης και ταξινόμησης των ιατρικών πράξεων, το οποίο διαφέρει ανάμεσα στις χώρες

- μια λίστα με διαφορετικές, πεπερασμένες, κατηγορίες (κωδικούς), οι οποίες θα αναφέρονται σε όμοιες, από πλευράς διάγνωσης και ανάλωσης πόρων, περιπτώσεις ασθενών

- ένας αλγόριθμος ταξινόμησης, διαθέσιμος και σε λογισμικό, ο οποίος να αντιστοιχεί σε διαφορετικούς συνδυασμούς διαγνώσεων (μπορεί να είναι πολλές), ιατρικών πράξεων (μπορεί να είναι πολλές), ηλικιών, φύλου, στις ομοιογενείς κατηγορίες,

- ένα σύστημα κοστολόγησης και καθορισμού αποζημίωσης που θα λαμβάνει υπόψη τις ιδιαιτερότητες των νοσοκομείων (πανεπιστημιακά) και των ασθενών (βαρύτητα, επιπλοκές, σπάνια περιστατικά) και τέλος

- ένα διοικητικό σύστημα εφαρμογής στα νοσοκομεία και ελέγχου από τους ασφαλιστικούς φορείς [11]. ”

Το ΥΥΚΑ έχει δημιουργήσει μια διαδικτυακή εφαρμογή για την εύκολη εύρεση των ΚΕΝ από τους εργαζόμενους στην υγεία. Η εφαρμογή αυτή αντιστοιχίζει τις διαγνώσεις εξόδου των ασθενών, οι οποίες είναι κωδικοποιημένες κατά ICD-10 καθώς και τις Ιατρικές πράξεις, οι οποίες είναι κωδικοποιημένες σύμφωνα με την κωδικοποίηση του ΚΕΣΥ, με τους κωδικούς των ΚΕΝ. Έτσι αν ο υπάλληλος του λογιστηρίου ασθενών εισάγει στην εφαρμογή τους κωδικούς ICD-10 (υποχρεωτικά) και τους κωδικούς Ιατρικών Πράξεων (προαιρετικά), η εφαρμογή του δίνει τον κωδικό ΚΕΝ που αντιστοιχεί σε αυτές. Η εφαρμογή ονομάζεται **Σύστημα Αντιστοίχησης Κωδικοποιήσεων (ΣΑΚ)** [12].

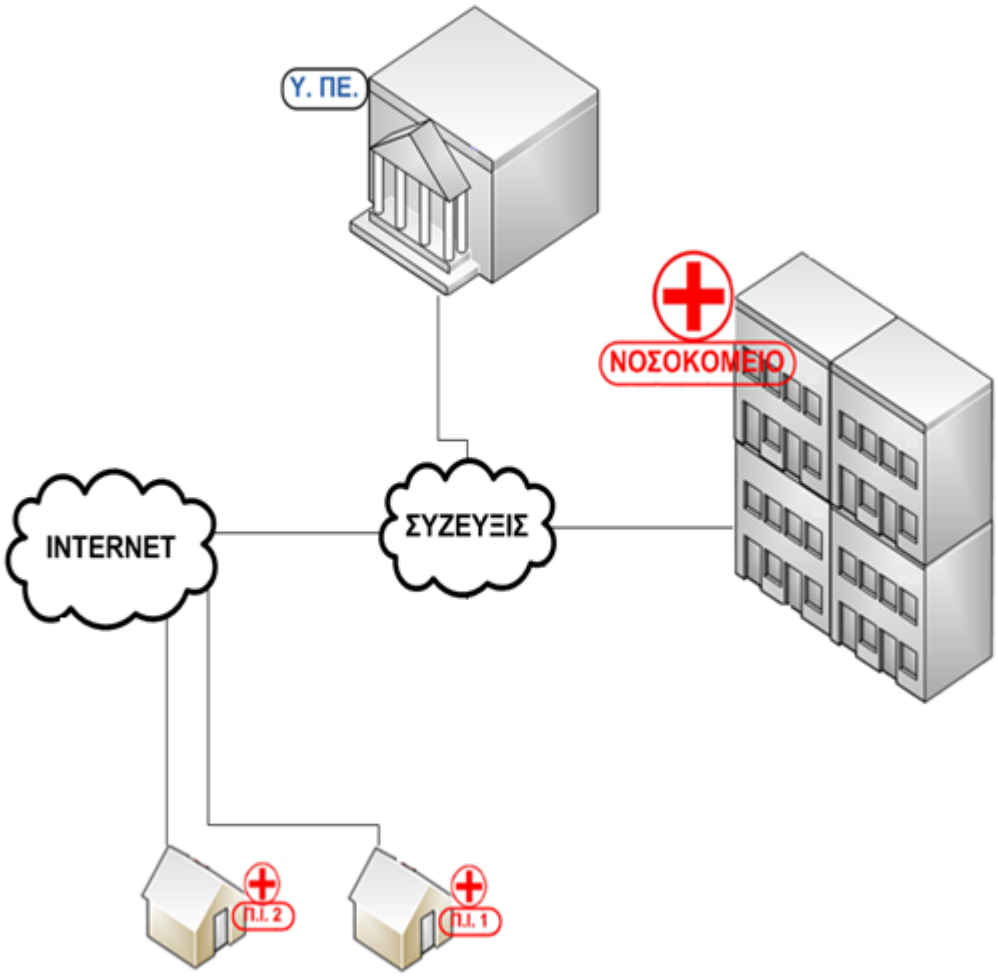
1.3 Τρέχουσα κατάσταση

Στην προσπάθεια ανάπτυξης των Τ.Π.Ε. στη δημόσια υγεία, το Υ.Υ.Κ.Α. σε τακτά χρονικά διαστήματα διενεργεί ελέγχους και αξιολόγηση της προόδου των έργων. Έτσι από την αξιολόγηση που διεξήχθη στις 7/3/12, τα επιμέρους πληροφοριακά συστήματα που αναπτύσσονται στα ελληνικά νοσοκομεία και αποτελούν το ΟΠΣΥ – και είναι σε διάφορα στάδια υλοποίησης – βλέπουμε πως είναι τα εξής [08]:

1. Διαχείριση Φαρμακείου
2. Διαχείριση Υλικών – Αποθήκες – Προμήθειες
3. Διαχείριση Υλικών – Αποθήκες
4. Γραφείο Προμηθειών (Διασύνδεση με διαχειρίσεις)
5. Λογιστήριο Ασθενών – Γραφείο Κίνησης – Κλειστό Ενοποιημένο Νοσήλιο (ΚΕΝ)
6. Διαχείριση Λογιστηρίου Ασθενών – ΚΕΝ
7. Διαχείριση Γραφείου Κίνησης
8. Τακτικά Εξωτερικά Ιατρεία (ΤΕΙ) – Τμήμα Επειγόντων Περιστατικών (ΤΕΠ) – Απογευματινά Ιατρεία (ΑΙ)
9. Διαχείριση ΤΕΙ – ΤΕΠ - ΑΙ
10. Γενικό Λογιστήριο – Διπλογραφικό – Μητρώο Δεσμεύσεων –Αναλυτική Λογιστική
11. Διαχείριση Γενικού Λογιστηρίου – Διπλογραφικού Συστήματος
12. Μητρώο Δεσμεύσεων
13. Αναλυτική Λογιστική
14. Διαχείριση Προσωπικού – Μισθοδοσία
15. Διαχείριση Προσωπικού
16. Διαχείριση Τακτικής Μισθοδοσίας
17. Διαχείριση Επικουρικής Μισθοδοσίας
18. Διαχείριση Κλινικών – Χρεώσεις
19. Διαχείριση Κλινικών – Παραπομπές – Ατομικό Συνταγολόγιο
20. Διαχείριση Κλινικών – Παραγγελία Υλικού
21. Χρεωστικός Φάκελος Ασθενή
22. Laboratory Information System (LIS) – Radiology Information System (RIS)
23. LIS
24. RIS
25. Διοικητική Πληροφορία (Management Information System – MIS)
26. Ιατρονοσηλευτικός Φάκελος

Κεφάλαιο 2
Το «HOSPITAL»

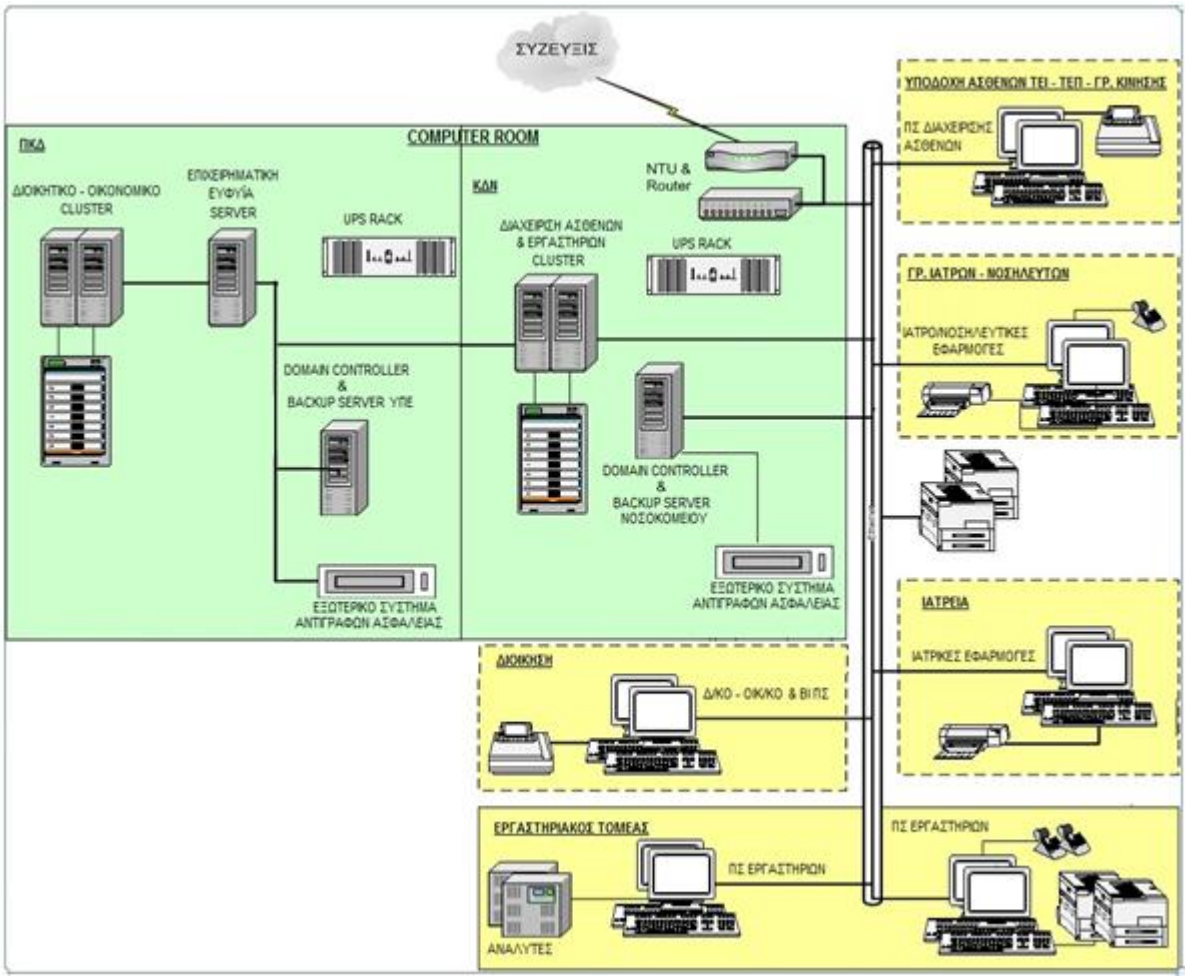
Το νοσοκομείο «HOSPITAL» έχει δύναμη 150 κλινών. Ανήκει διοικητικά στην Υ.Πε. και σε αυτό ανήκουν διοικητικά δύο Περιφερειακά Ιατρεία. Η τηλεπικοινωνιακή διασύνδεση του νοσοκομείου με τις υπόλοιπες διοικητικές δομές της ιεραρχίας έως το 3ο επίπεδο και με το διαδίκτυο φαίνεται στην εικόνα 2.1.



Εικόνα 2.1: Τηλεπικοινωνιακή σύνδεση «HOSPITAL»

2.1 Αρχιτεκτονική ΟΠΣΥ - ΟΠΣΝ

Η υλοποίηση του ΟΠΣΥ γίνεται στο «HOSPITAL». Σε αυτό συνδέονται τα υπόλοιπα νοσοκομεία, τα κέντρα υγείας και η διοίκηση της Υ.ΠΕ., μέσω του «ΣΥΖΕΥΞΙΣ». Αντίθετα τα Π.Ι. που ανήκουν στο «HOSPITAL» έχουν αυτόνομους (stand alone) Η/Υ που συνδέονται στο διαδίκτυο μέσω παρόχων ADSL σύνδεσης. Η αρχιτεκτονική του δικτύου φαίνεται στην εικόνα 2.2.



Εικόνα 2.2: Αρχιτεκτονική δικτύου του «HOSPITAL»

Το ΟΠΣΥ αποτελείται από:

1. **Το Περιφερειακό Κέντρο Δεδομένων – ΠΚΔ**, με εξοπλισμό που εξυπηρετεί όλη την Υ.ΠΕ. Σε αυτό υπάρχουν οι Πληροφοριακές Υποδομές Υγείας της Υ.ΠΕ. και το σύστημα Πρωτοβάθμιας Φροντίδας Υγείας (Διαχείριση Ασθενών και Ιατρικές Εφαρμογές Κ.Υ.). Υλοποιείται από:

   1.1. Μία συστοιχία (cluster) δύο servers για το Διοικητικό – Οικονομικό υποσύστημα. Αυτοί έχουν την βάση δεδομένων (database) και τους εξυπηρετητές εφαρμογών (application servers) σε διάταξη cluster active (λειτουργούν ταυτόχρονα εφαρμογές και βάση δεδομένων) και βρίσκονται σε διάταξη καταμερισμού φόρτου (load balancing).

   1.2. Ένας server για το υποσύστημα Επιχειρηματικής Ευφυΐας (Business Intelligence – BI).

   1.3. Ένας server που εκτελεί εργασίες Domain Controller και Backup Server.

1.4. Κοινός, εξωτερικός, αποθηκευτικός χώρος με τον οποίο οι servers έχουν διπλές οδεύσεις για υψηλή διαθεσιμότητα.

2. **Το Κέντρο Δεδομένων του Νοσοκομείου – ΚΔΝ**, στο οποίο υπάρχουν τα Πληροφοριακά Υποσυστήματα του νοσοκομείου μαζί με τα υποσυστήματα Διαχείρισης Ασθενών, Ιατρικές Εφαρμογές, και τα Πληροφοριακά Συστήματα Εργαστηρίων – ΠΣΕ. Υλοποιείται από:

   2.1. Μία συστοιχία (cluster) δύο servers για το υποσύστημα Διαχείρισης Ασθενών και το υποσύστημα των Εργαστηρίων με τα Υποσυστήματα:

   - Διαμεσολαβητής Μηνυμάτων (ΔΜ - Rhapsody)
   - Διαχείρισης Ασθενών
   - Ιατρικών Εφαρμογών
   - Πληροφοριακό Σύστημα Εργαστηρίων

   2.2. Ένας server που εκτελεί εργασίες Domain Controller και Backup Server.

   2.3. Κοινός, εξωτερικός, αποθηκευτικός χώρος.

3. **Τους πελάτες (clients)** που χρησιμοποιούν τα υποσυστήματα με λειτουργικά συστήματα Windows XP ή Windows 7.

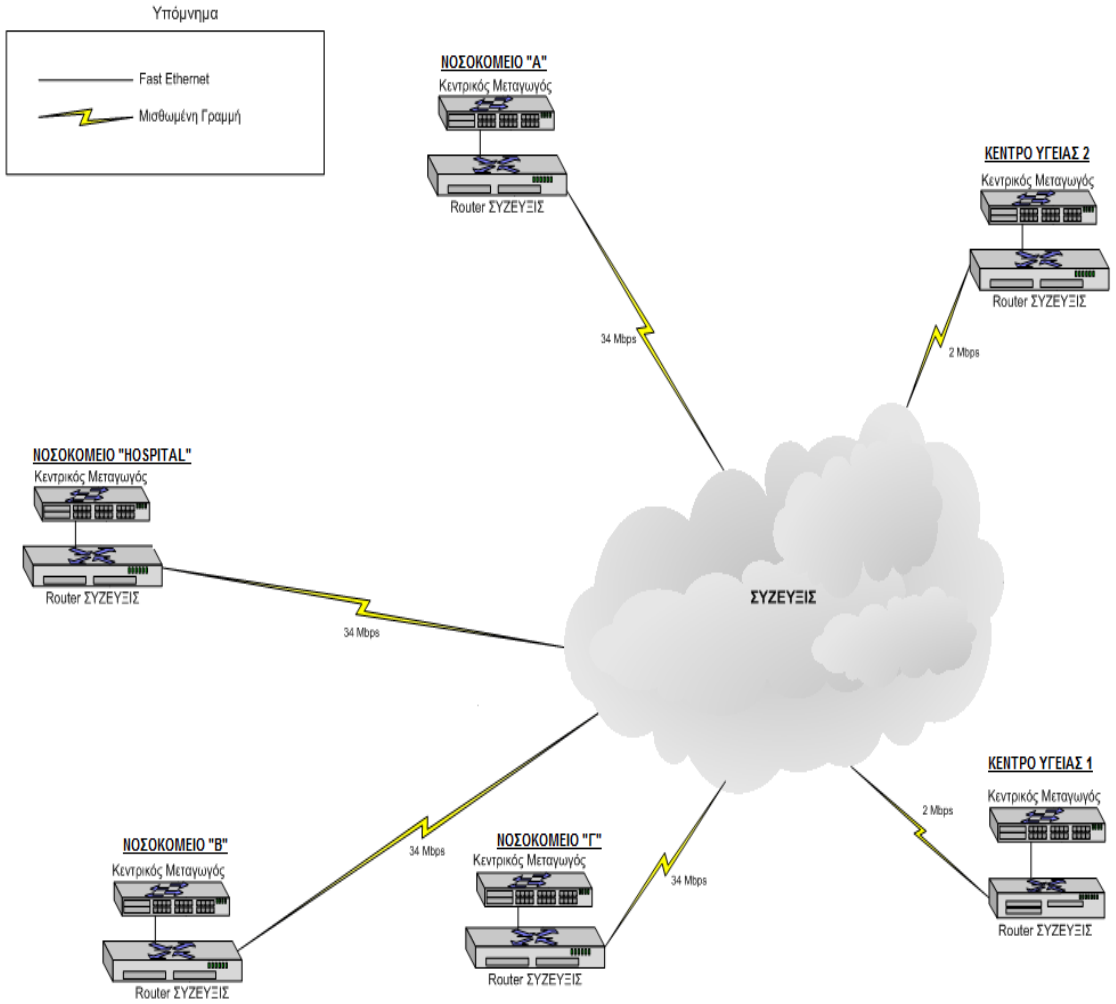
4. **Αυτόνομες εφαρμογές**, που υπάρχουν σε stand alone Η/Υ και εξυπηρετούν διάφορες ανάγκες του νοσοκομείου.

5. **Τους Η/Υ των Π.Ι.** οι οποίοι χρησιμοποιούνται για ηλεκτρονική συνταγογράφηση (e-syntagografisi) και ηλεκτρονική παραγγελία εξετάσεων (e-diagnosis).

6. **Τα cluster** υλοποιούνται από το λειτουργικό σύστημα Windows 2003 Enterprise Edition και από την βάση δεδομένων Microsoft SQL Server 2000, ενώ για τους πελάτες (clients) των υπηρεσιών όλο το cluster εμφανίζεται ως ένας υπολογιστής.

2.2 Αρχιτεκτονική Δικτύου

Η δικτυακή διασύνδεση όλων των μονάδων υγείας πραγματοποιείται μέσω του δικτύου ΣΥΖΕΥΞΙΣ. Η φυσική διασύνδεση πραγματοποιείται μέσω εγκατεστημένων δρομολογητών. Το δίκτυο ευρείας περιοχής (WAN) που δημιουργήθηκε έχει την δυνατότητα να μεταφέρει παράλληλα με τα δεδομένα και υπηρεσίες φωνής. Η διασύνδεση με τα τοπικά δίκτυα (LAN) των μονάδων υγείας πραγματοποιείται με σύνδεση Fast Ethernet, μεταξύ των δρομολογητών του ΣΥΖΕΥΞΙΣ και των κεντρικών μεταγωγών της κάθε μονάδας υγείας. Στην εικόνα 2.4 που ακολουθεί εμφανίζονται οι διασυνδέσεις.



Εικόνα 2.4: Αρχιτεκτονική Δικτύου WAN

2.2.1 Διασύνδεση Ενεργού Εξοπλισμού

Η αρχιτεκτονική του δικτύου στο «HOSPITAL» είναι τύπου «ανεπτυγμένο δίκτυο κορμού (collapsed backbone)». Οι συνδέσεις του κεντρικού μεταγωγού (router) με τους υπόλοιπους μεταγωγούς πραγματοποιείται με ταχύτητα 1 gigabit, ενώ στους τελικούς χρήστες η σύνδεση γίνεται με Fast Ethernet 100 Mbps. Το Backbone του εσωτερικού δικτύου είναι Gigabit Ethernet. Κάθε server επικοινωνεί με το τοπικό δίκτυο με διπλές κάρτες Gigabit Ethernet για λόγους απόδοσης και υψηλής διαθεσιμότητας.

Στον **υπόγειο** του νοσοκομείου, στο ΠΚΔ, έχουν εγκατασταθεί τέσσερις **κεντρικοί** μεταγωγοί που καλύπτουν τις συνδέσεις με τον υπόλοιπο προσφερόμενο ενεργό εξοπλισμό στους ορόφους καθώς και με τους servers. Επίσης τρεις μεταγωγοί σε διάταξη stack που καλύπτουν τις ανάγκες δικτύωσης του χώρου.

Οι ανάγκες δικτύωσης του **ισογείου** καλύπτονται από πέντε μεταγωγούς σε διάταξη stack.

Στον **πρώτο όροφο** έχουν εγκατασταθεί τέσσερις κατανεμητές, με δύο μεταγωγούς σε διάταξη stack.

Οι ανάγκες δικτύωσης του **δεύτερου ορόφου καλύπτονται από δυο** μεταγωγούς σε διάταξη stack

Οι ανάγκες δικτύωσης του **τρίτου ορόφου** καλύπτονται από δυο μεταγωγούς σε διάταξη stack.

Τα stack των ορόφων συνδέονται με τον κεντρικό μεταγωγό μέσω μιας οπτικής ίνας, σύνδεσης 1000Base-SX.

2.2.2 Κωδικοποιήσεις

Οι διεθνείς και εθνικές κωδικοποιήσεις και ορολογίες που χρησιμοποιούνται είναι οι ακόλουθες:

- Γενικές βιβλιοθήκες κωδικοποιημένων στοιχείων (π.χ. φύλο, είδος διεύθυνσης, χώρα κατά ISO 3166, ημέρα της εβδομάδας, γλώσσα κατά ISO 639, κατάσταση μίας παραγγελίας, προέλευση ενός δείγματος, είδος τηλεπικοινωνιακού εξοπλισμού, κλπ).
- Κωδικοποίηση λογιστικού σχεδίου – κωδικών προϋπολογισμού (ΚΑΕ) με βάση το Προεδρικό Διάταγμα 146 (ΦΕΚ 122/21-05-2003).

- Υπηρεσίες που παρέχονται από τα διάφορα κέντρα κόστους, μαζί με το κόστος τους.
- Υφιστάμενες κωδικοποιήσεις αναφορικά με τους πόρους (π.χ. υλικά, φάρμακα, αντιδραστήρια κλπ) που κάθε κέντρο κόστους χρησιμοποιεί για την παροχή των υπηρεσιών του
- Διεθνής Ταξινόμηση Πρωτοβάθμιας Φροντίδας Υγείας (ICPC),
- Διεθνής Στατιστική Ταξινόμηση Ασθενειών και Σχετικών Προβλημάτων Υγείας (ICD-10),
- Κωδικοποίηση και Ονοματολογία Εργαστηριακών Παρατηρήσεων (LOINC),
- Κωδικοποιήσεις του Υπουργείου Οικονομικών,
- Κωδικοποίηση λογιστικού σχεδίου – κωδικών προϋπολογισμού (ΚΑΕ)
- Κωδικοποίηση Ιατρικών Πράξεων του Κεντρικού Συμβουλίου Υγείας,
- Κωδικοποιήσεις του ISO (αναφορικά με γλώσσα & εθνικότητα),
- Κωδικοποιήσεις του Χάρτη Υγείας και Πρόνοιας της Ελλάδας,
- Κωδικοποίηση/ ταξινόμηση των φαρμάκων του Εθνικού Οργανισμού Φαρμάκων και κατά ATC (Anatomical Therapeutic Chemical),
- Κωδικοποίηση με βάση το Διεθνές Πρότυπο Ονοματολογίας Ιατροτεχνολογικού Εξοπλισμού (UMDNS του ECRI και GMDN του CEN TC257),
- HL7

2.2.3 Διασυνδέσεις Συστημάτων

Η διασυνδεσιμότητα μεταξύ των εφαρμογών όλων των μονάδων υγείας στο εσωτερικό της ΥΠΕ γίνεται:

1. μέσω ανταλλαγής μηνυμάτων και του προτύπου HL7
2. μέσω πρόσβαση σε κοινές πληροφοριακές υποδομές (π.χ. ΥΤΑ)
3. μέσα από το σύστημα επιχειρηματικής ευφυΐας

Βασικό συστατικό αποτελεί ο Διαμεσολαβητής Μηνυμάτων (ΔΜ – MB) Rhapsody, ο οποίος υποστηρίζει την αυτοματοποίηση λειτουργικά κρίσιμων διαδικασιών που απαιτούν την ανταλλαγή πολύμορφων δεδομένων:

1. στο εσωτερικό ενός φορέα υγείας
2. μεταξύ των φορέων υγείας μίας ΥΠΕ

Οι διασυνδέσεις που υποστηρίζονται είναι οι εξής:

1. διασύνδεση υποσυστήματος διαχείρισης ασθενή (λογιστήριο ασθενή) με διοικητικο-οικονομικό υποσύστημα (ενημέρωση λογιστικής)
2. διασύνδεση υποσυστήματος διαχείρισης ασθενή (εφαρμογή κλινικής-ορόφου) με φαρμακείο
3. διασύνδεση υποσυστήματος διαχείρισης ασθενή (εφαρμογή κλινικής-ορόφου) με διαιτολογικό
4. διασύνδεση υποσυστήματος διαχείρισης ασθενή με υπηρεσία ταυτοποίησης ασθενή
5. διασύνδεση υποσυστήματος διαχείρισης ασθενή (εφαρμογή κλινικής-ορόφου) με πληροφοριακό σύστημα εργαστηρίου
6. Η διασύνδεση του υποσυστήματος ΔΑ/ΙΥ με το Διοικητικοοικονομικό Πληροφοριακό Σύστημα (ΔΟ) επιτυγχάνεται με την ανταλλαγή αρχείων σε μορφή **XML (Extensible Markup Language).** Όταν ολοκληρώνεται μία χρέωση για έναν ασθενή από το υποσύστημα ΔΑ/ΙΥ, δημιουργείται ένα αρχείο σε μορφή XML το οποίο περιέχει το σύνολο της πληροφορίας για τη χρέωση του ασθενή (απόδειξη ασθενή). Το αρχείο αυτό αποστέλλεται στο ΔΟ, το οποίο καταγράφει τα δεδομένα της εκάστοτε χρέωσης. Αποτελείται από τα εξής τμήματα πληροφορίας:

   6.1. Στοιχεία Απόδειξης

   6.1.1. Κωδικός Συστήματος για το Περιστατικό (εισαγωγή ή επίσκεψη)

   6.1.2. Ημερομηνίες Απόδειξης, Εισαγωγής και Εξόδου

   6.2. Στοιχεία Ασθενή

   6.2.1. Περιγράφονται στοιχεία ταυτοποίησης, δημογραφικά (π.χ. ονοματεπώνυμο ασθενούς, Φορολογικά Στοιχεία, Δ/νση κ.α.)

   6.3. Στοιχεία Υπηρεσιών που χρεώθηκαν

   6.3.1. Περιγραφή Υπηρεσίας, ποσότητα, τιμή, συμμετοχή ασθενή, πληρωτέα ποσά κ.α.

6.4. Συνολική Αναφορά

6.4.1. Αναφέρονται συνολικά τα δεδομένα χρέωσης που περιγράφει η απόδειξη

2.2.4 Διαχείριση Ηλεκτρονικού Φακέλου Ασθενή - ΗΦΑ

Στη διαχείριση του ΗΦΑ έχουν πρόσβαση τα παρακάτω εμπλεκόμενα τμήματα του νοσοκομείου μέσω των αντίστοιχων συστημάτων τους:

1. Η Γραμματεία Εξωτερικών Ιατρείων
2. Η Γραμματεία Απογευματινών Ιατρείων,
3. Το Γραφείο Κίνησης,
4. Το Λογιστήριο Ασθενών
5. Η Γραμματεία ΤΕΠ
6. Οι Κλινικές/ Όροφοι.

Η πρόσβαση στις λειτουργικότητες του ΗΦΑ **εξαρτάται από την κάθε λειτουργική περιοχή και το ρόλο των χρηστών.** Για παράδειγμα, το Γραφείο Κίνησης μπορεί να ανοίγει ή και να δημιουργεί τον ηλεκτρονικό φάκελο ασθενή και να έχει πρόσβαση σε δημογραφικά και ασφαλιστικά δεδομένα, όχι όμως στα ιατρικά δεδομένα.

Από την στιγμή που δημιουργηθεί για πρώτη φορά ο ηλεκτρονικός φάκελος του ασθενή, στο Σύστημα Νοσοκομείου τότε σε κάθε άλλη επαφή του ασθενή με το νοσοκομείο δεν καταγράφονται πάλι τα δημογραφικά και ασφαλιστικά του στοιχεία αλλά αφού γίνει η ταυτοποίηση του ασθενή, ανοίγει ο ηλεκτρονικός φάκελος του ασθενή και οι διάφοροι χρήστες, ανάλογα και με τα δικαιώματα πρόσβασης που έχουν, καταγράφουν τα δεδομένα που δημιουργούνται στα πλαίσια της συγκεκριμένης επαφής.

Οι βασικές λειτουργικότητες σχετικά με την διαχείριση του ηλεκτρονικού φακέλου ενός ασθενή είναι οι εξής:

1. Διαχείριση καρτέλας ασθενή: Αναζήτηση καρτέλας ασθενή, ταυτοποίηση - ενιαίος αριθμός μητρώου ασθενή, δημιουργία καρτέλας ασθενή, ενημέρωση δημογραφικών δεδομένων, συγχώνευση φακέλων, διαχείριση διπλοεγγραφών

2. Δημιουργία περιστατικού και κωδικού περιστατικού
3. Προσθήκη στοιχείων στον φάκελο υγείας του ασθενή:
4. Διαγνώσεις: Περιλαμβάνει τις διαγνώσεις που αφορούν τον ασθενή (Διάγνωση Εισόδου – Εξόδου - Υπό διερεύνηση).
5. Διαγνωστικές Πράξεις: Περιλαμβάνει όλες τις ιατρικές πράξεις – εξετάσεις που γίνονται για να διαγνωσθεί η κλινική κατάσταση του ασθενούς.
6. Θεραπευτικές Πράξεις: Περιλαμβάνει όλες τις ιατρικές πράξεις για την αντιμετώπιση της κατάστασης του ασθενούς.
7. Ιατρικές Αναφορές: Περιλαμβάνει όλες τις γνωματεύσεις – εκθέσεις – ενημερωτικά που αφορούν τον ασθενή.
8. Ιστορικό: Περιλαμβάνει όλες τις πληροφορίες για το ιατρικό ιστορικό του ασθενή.
9. Πορεία Νόσου: Περιλαμβάνει τις πληροφορίες για την πορεία νόσου του ασθενή κατά την παρούσα νοσηλεία του.
10. Ιατρικές Οδηγίες για νοσηλευόμενο ασθενή
11. Καταγραφή νοσηλευτικών πράξεων στα πλαίσια εκτέλεσης ιατρικών οδηγιών (μετρήσεις ζωτικών, υγρά, χορήγηση φαρμακευτικής αγωγής, διενέργεια εξετάσεων κλπ)
12. Παραγγελίες εξετάσεων – παραλαβή εργαστηριακών αποτελεσμάτων
13. Παραγγελίες φαρμάκων ατομικού συνταγολογίου
14. Παραγγελία δίαιτας
15. Παραγγελίες υγειονομικού υλικού με ατομική χρέωση στον ασθενή
16. Κίνηση ασθενή (εισαγωγή, μεταφορά, έξοδος)
17. Προγραμματισμός παροχής υπηρεσιών υγείας (εισαγωγή σε τμήμα, επίσκεψη σε εξωτερικό ιατρείο, εργαστηριακή εξέταση)

2.2.5 Υποσυστήματα του «HOSPITAL»

Τα υποσυστήματα του «HOSPITAL» είναι:

1. Ιατρονοσηλευτικό στο ΚΔΝ
2. Διαχείρισης Ασθενή στο ΚΔΝ
3. Διαχείριση Ραντεβού σε εξωτερικό συνεργάτη
4. Διοικητικο-Οικονομικό στο ΠΚΔ
5. Πληροφοριακό Σύστημα Εργαστηρίου στο ΚΔΝ
6. Business Intelligence στο ΠΚΔ

Ιατρονοσηλευτικό Υποσύστημα - ΙΥ

Αποτελείται από τα εξής υποσυστήματα:

1. **Σύστημα Εξωτερικών/Απογευματινών Ιατρείων**

   Στα πλαίσια της διαχείρισης της επίσκεψης ασθενή στο ιατρείο, στα Εξωτερικά/Απογευματινά Ιατρεία οι γιατροί – χρήστες χρησιμοποιούν του Η/Υ για την ηλεκτρονική συνταγογράφηση και την ηλεκτρονική παραγγελία εξετάσεων.

2. **Σύστημα ΤΕΠ**

   Η διαχείριση επείγοντος περιστατικού από το Σύστημα των ΤΕΠ δεν διαφέρει από την διαχείριση επίσκεψης στα εξωτερικά ιατρεία από το Σύστημα Εξωτερικών Ιατρείων. Υποστηρίζονται η ηλεκτρονική συνταγογράφηση και η ηλεκτρονική παραγγελία εξετάσεων.

3. **Σύστημα Κλινικής/ορόφου**

   Το Σύστημα της Κλινικής /ορόφου υποστηρίζει όλες τις διαδικασίες που διεκπεραιώνονται από το προσωπικό μιας κλινικής/ ορόφου (ιατρικό, νοσηλευτικό, διοικητικό) στα πλαίσια της καθημερινής διαχείρισης και παρακολούθησης των εσωτερικών ασθενών ατομικά ή του τμήματος συνολικά. Για κάθε νοσηλεία του ασθενή σε κάποια κλινική, το σύστημα δημιουργεί στον ηλεκτρονικό φάκελο του ασθενή, τον αντίστοιχο φάκελο περιστατικού για την νοσηλεία και δίνει έναν μοναδικό κωδικό για την συγκεκριμένη επαφή. Ο φάκελος

περιστατικού περιλαμβάνει όλα τα δεδομένα που καταγράφονται στα πλαίσια της λογοδοσίας του ιατρικού και νοσηλευτικού προσωπικού καθώς και στα πλαίσια της διεκπεραίωσης των υπόλοιπων διαδικασιών διαχείρισης του ασθενή (πχ. παραγγελίες εξετάσεων-παραλαβή αποτελεσμάτων κλπ). Η βασική διαδικασία που υποστηρίζεται από το σύστημα είναι η διαδικασία διαχείρισης νοσηλευομένου ασθενή. Η συνολική διαδικασία διαχείρισης νοσηλευομένου ασθενή αποτελείται από κάποια βασικά στάδια καθένα από τα οποία περιλαμβάνει ένα σύνολο από βασικές ή εναλλακτικές διαδικασίες. Αυτά είναι τα εξής:

3.1. Διαχείριση εισαγωγής: Για το πρώτο στάδιο υπάρχουν τέσσερα εναλλακτικά σενάρια όσο αφορά την ενεργοποίηση της εισαγωγής και την διεκπεραίωσή της:

3.1.1. Διαχείριση προγραμματισμένης εισαγωγής,

3.1.2. Διαχείριση επείγουσας εισαγωγής,

3.1.3. Διαχείριση απευθείας εισαγωγής στην κλινική, και

3.1.4. Διαχείριση απευθείας εισαγωγής από το Γραφείο Κίνησης.

Στα πλαίσια των παραπάνω γίνεται η έκδοση του εισιτήριου και η ανάθεση του ασθενή στην κλινική ενώ υπάρχει η επικοινωνία του Συστήματος Κλινικής με το Σύστημα του Γραφείου Κίνησης ή το Σύστημα Επειγόντων.

3.2. Διαχείριση νοσηλευομένου ασθενή στην κλινική: Στην συνέχεια και αφού ολοκληρωθεί η εισαγωγή του ασθενή στην κλινική, κατά το στάδιο της νοσηλείας του υποστηρίζονται ένα σύνολο από βασικές λειτουργίες για αντίστοιχες διαδικασίες:

3.3. Πρόσβαση-ενημέρωση του ιστορικού του ασθενή.

3.4. Οδηγίες-λογοδοσία: περιλαμβάνει τις οδηγίες του ιατρικού προσωπικού προς το νοσηλευτικό, την διενέργεια ιατρικών και νοσηλευτικών πράξεων, τις χορηγήσεις φαρμάκων-υγειονομικού υλικού, τις μετρήσεις ζωτικών, την σίτιση και λοιπές ενέργειες.

3.5. Παραγγελίες εξετάσεων-παραλαβή αποτελεσμάτων

3.6. Παραγγελίες φαρμάκων-υγειονομικού υλικού στο φαρμακείο-αποθήκη του νοσοκομείου-παραλαβή

3.7. Παραγγελίες άλλων υλικών στην αποθήκη του νοσοκομείου-παραλαβή

3.8. Παραγγελίες δίαιτας

3.9. Διαχείριση μεταφοράς.

3.10. Έναρξη διαδικασίας εξόδου ασθενή από την κλινική: η διαδικασία εξόδου ξεκινάει από την κλινική με την συγγραφή του εξιτηρίου και του ενημερωτικού σημειώματος για τον ασθενή, συνεχίζει στο Λογιστήριο Ασθενών με την τιμολόγηση- εκκαθάριση του λογαριασμού του ασθενή, και τελειώνει στο Γραφείο Κίνησης με την επικύρωση του εξιτηρίου και την έξοδο του ασθενή. Για λόγους ελέγχου της τακτοποίησης των οικονομικών της νοσηλείας από τον ασθενή, η διαδικασία εξόδου μπορεί να τελειώνει με την ενημέρωση της κλινικής από το Γραφείο Κίνησης και την απόδοση στον ασθενή του ενημερωτικού σημειώματος. Για το στάδιο αυτό υποστηρίζονται οι ακόλουθες λειτουργίες:

3.10.1. Δημιουργία/ καταγραφή/εκτύπωση ενημερωτικού σημειώματος

3.10.2. Δημιουργία/ καταγραφή/ εκτύπωση εξιτηρίου

3.10.3. Ενημέρωση πλάνου ορόφου: ο χρήστης ελευθερώνει το κρεβάτι του ασθενή από το πλάνο ορόφου.

3.10.4. Αυτόματη ενημέρωση Συστήματος Λογιστηρίου Ασθενών: Το Σύστημα Λογιστηρίου, ως τμήμα του Συστήματος Νοσοκομείου, έχει πρόσβαση σε ορισμένα από τα δεδομένα του φακέλου όπως τα δημογραφικά-ασφαλιστικά δεδομένα του ασθενή και όλα τα δεδομένα που χρειάζονται για την χρέωση του ασθενή

3.11. Τέλος στα πλαίσια της συνολικής διαχείρισης της κλινικής/ορόφου από το νοσηλευτικό προσωπικό υποστηρίζονται τα εξής:

3.11.1. Παραγγελία φαρμάκων γενικού συνταγολογίου

3.11.2. Παραγγελία υγειονομικού υλικού, αναλωσίμων για το τμήμα

3.11.3. Παραγγελία διαιτολογίου

3.11.4. Συνολική παρακολούθηση παραγγελιών τμήματος (κατάσταση παραγγελιών που έγιναν, εκκρεμείς παραγγελίες)

3.11.5. Διαχείριση πλάνου ορόφου

3.11.6. Αναφορές Νοσηλευτικής Υπηρεσίας (ημερήσια κίνηση κλπ)

Υποσύστημα Διαχείρισης Ασθενή - ΔΑ

Το ΔΑ περιλαμβάνει τις εξής λειτουργικότητες:

1. **Διαχείριση καρτέλας ασθενή.**

   Αναζήτηση καρτέλας ασθενή, ταυτοποίηση - ενιαίος αριθμός μητρώου ασθενή, δημιουργία καρτέλας ασθενή, δημιουργία καρτέλας αγνώστου ασθενή, ενημέρωση δημογραφικών δεδομένων, συγχώνευση φακέλων, διαχείριση διπλοεγγραφών

2. **Δημιουργία περιστατικού και κωδικού περιστατικού**

Αποτελείται από τα εξής υποσυστήματα:

1. **Σύστημα Γραμματείας Εξωτερικών Ιατρείων**

   Το Σύστημα της Γραμματείας Εξωτερικών Ιατρείων περιλαμβάνει τις λειτουργικότητες δύο βασικών υποσυστημάτων.

   1.1. **Του Συστήματος Διαχείρισης Ραντεβού**: Η Γραμματεία των Εξωτερικών Ιατρείων τηρεί τη λίστα αναμονής των ασθενών για επισκέψεις στα Εξωτερικά ή Απογευματινά Ιατρεία, μέσω της διασύνδεσης με την εταιρεία που παρέχει το σύστημα διαχείρισης

ραντεβού. Επίσης μπορεί να κλείνει και αυτόνομα ραντεβού που ζητούν οι πολίτες με τη χρήση του ίδιου συστήματος.

1.2. **Του Συστήματος Λογιστηρίου Ασθενών**: για την περίπτωση της Γραμματείας Εξωτερικών Ιατρείων ο χρήστης έχει πρόσβαση στις λειτουργικότητες του Λογιστηρίου Ασθενών που αφορούν την τιμολόγηση του εξωτερικού ασθενή και την έκδοση της σχετικής απόδειξης. Επίσης έχει πρόσβαση στις λειτουργικότητες σχετικά με τις υποβολές στα ασφαλιστικά ταμεία για τους εξωτερικούς ασθενείς.

2. Σύστημα Γραμματείας Απογευματινών Ιατρείων

Στο Σύστημα της Γραμματείας Απογευματινών Ιατρείων οι χρήστες ανάλογα με τα δικαιώματα το ρόλου τους, μπορούν να έχουν πρόσβαση στις λειτουργικότητες του Λογιστηρίου Ασθενών που αφορούν την χρέωση του εξωτερικού ασθενή και την έκδοση της σχετικής απόδειξης και στη διαχείριση του μεριδολογίου.

3. Σύστημα Γραμματείας ΤΕΠ

Το Σύστημα της Γραμματείας ΤΕΠ περιλαμβάνει τις εξής λειτουργικότητες:

3.1. Διαχείριση καρτέλας ασθενή: Αναζήτηση καρτέλας ασθενή, ταυτοποίηση - ενιαίος αριθμός μητρώου ασθενή, δημιουργία καρτέλας ασθενή, δημιουργία καρτέλας αγνώστου ασθενή, ενημέρωση δημογραφικών δεδομένων, συγχώνευση φακέλων, διαχείριση διπλοεγγραφών

3.2. Δημιουργία περιστατικού και κωδικού περιστατικού

3.3. Τιμολόγηση ασθενή για εργαστηριακές εξετάσεις

4. Σύστημα Γραφείου Κίνησης

Το Σύστημα του Γραφείου Κίνησης υποστηρίζει την παρακολούθηση της πορείας του εσωτερικού (νοσηλευόμενου) ασθενή και όλες του τις μετακινήσεις κατά τα διάφορα στάδια της νοσηλείας του, από την εισαγωγή του έως και έξοδό του από το νοσοκομείο με την έκδοση εξιτηρίου. Υποστηρίζει τη δημιουργία του φακέλου ασθενή, εφόσον αυτός δεν υπάρχει ήδη στο σύστημα, με την καταγραφή των δημογραφικών και ασφαλιστικών

στοιχείων ενώ στην συνέχεια γίνεται η καταγραφή των υπόλοιπων στοιχείων της εισαγωγής. Οι βασικές λειτουργικότητες του Συστήματος Γραφείου Κίνησης είναι οι εξής:

4.1. **Διαχείριση εισαγωγής:** Για την διαχείριση της εισαγωγής ασθενή από το Γραφείο Κίνησης το σύστημα υποστηρίζει **εναλλακτικά σενάρια** που έχουν σχέση με το αν η εισαγωγή είναι προγραμματισμένη ή όχι, αλλά και με τον βαθμό αυτοματοποίησης των αντίστοιχων διαδικασιών. Συνοπτικά, υποστηρίζονται οι εξής περιπτώσεις:

4.2. Διαχείριση προγραμματισμένης εισαγωγής ασθενή.

Στα πλαίσια αυτού του σεναρίου υποστηρίζονται οι εξής λειτουργίες:

4.2.1. Αναζήτηση, ταυτοποίηση, και άνοιγμα του φακέλου του ασθενή

4.2.2. Δημιουργία περιστατικού και κωδικού περιστατικού

4.2.3. Δημιουργία, διόρθωση εισιτηρίου

4.2.4. Επικύρωση εισιτηρίου

4.2.5. Επιβεβαίωση εισαγωγής

4.2.6. Εκτύπωση εισιτηρίου

4.2.7. Ανάθεση ασθενή σε θάλαμο, κλίνη, καταγραφή υπόλοιπων στοιχείων

4.3. Διαχείριση επείγουσας εισαγωγής ασθενή.

Στην περίπτωση της επείγουσας εισαγωγής, η διαδικασία ξεκινάει από τα επείγοντα όπου καταγράφεται το εισιτήριο και η εντολή εισόδου του ασθενή. Το Γραφείο Κίνησης ενημερώνεται αυτόματα για την εισαγωγή.

4.4. Διαχείριση απευθείας εισαγωγής ασθενή σε κλινική.

Σε περιπτώσεις που ο ασθενής εισαχθεί απευθείας στην κλινική, χωρίς να περάσει από το Γραφείο Κίνησης η αναζήτηση, ταυτοποίηση και άνοιγμα ή δημιουργία του φακέλου

ασθενούς, αν χρειάζεται, και η καταγραφή του εισιτηρίου μπορεί να έχει γίνει στην κλινική. Στις περιπτώσεις αυτές που η εισαγωγή του ασθενή γίνεται στην κλινική, υπάρχει αυτόματη ενημέρωση του Γραφείου Κίνησης.

4.5. Διαχείριση μεταφοράς ασθενή.

Η διαχείριση μεταφοράς γίνεται από την κλινική και ενημερώνεται το Γραφείο Κίνησης αυτόματα. Εναλλακτικά ή και μαζί, όλες οι σχετικές ενέργειες όπως η **καταγραφή** των δεδομένων, η **ενημέρωση του πλάνου ορόφου** των εμπλεκόμενων κλινικών και οι **σχετικές εκτυπώσεις** μπορούν να γίνονται και από το Γραφείο Κίνησης το οποίο μπορεί να έχει πλήρη πρόσβαση στο πλάνο ορόφου κάθε κλινικής. Κατά την μετακίνηση ασθενή σε άλλη κλινική γίνεται αυτόματη προσαρμογή του φακέλου στα νέα δεδομένα όπως νέα νοσήλια, νέο συνταγολόγιο φαρμάκων, νέα λίστα εξετάσεων κλπ.

4.6. Διαχείριση εξόδου ασθενή**.**

Το Σύστημα του Γραφείου Κίνησης σε συνεργασία με το Σύστημα Λογιστηρίου Ασθενών υποστηρίζει την διαδικασία εξόδου ασθενή τόσο στην περίπτωση πλήρους αυτοματοποίησής της όσο και στην περίπτωση που όλα τα δεδομένα (εξιτήριο, δεδομένα για την χρέωση του ασθενή σχετικά με εξετάσεις, φάρμακα, υγειονομικό υλικό κλπ) μεταφέρονται έντυπα στο Γραφείο Κίνησης και το Λογιστήριο και καταχωρούνται στα αντίστοιχα συστήματα.

4.7. Διαχείριση Κλινών**.**

Το Σύστημα του Γραφείου Κίνησης υποστηρίζει την διαχείριση των κλινών όλων των κλινικών και τη δυνατότητα παρακολούθησης όλων των εσωτερικών μετακινήσεων των ασθενών. Οι χρήστες αποκτούν έτσι πλήρη εικόνα σχετικά με την πληρότητα του Νοσοκομείου και διαχειρίζονται τις κλίνες και θέσεις νοσηλείας του Νοσοκομείου

4.8. Εκτυπώσεις.

Το Σύστημα του Γραφείου Κίνησης υποστηρίζει την διαχείριση των εισιτηρίων και εξιτηρίων των Ασθενών όπως επίσης και η δημιουργία πολλαπλών εκτυπωτικών όπως είναι η έκδοση εισιτηρίων, εξιτηρίων, η έκδοση πιστοποιητικών νοσηλείας, εισαγωγής, εξαγωγής, βεβαιώσεις προς ασφαλιστική χρήση, κλπ.

5. Σύστημα Λογιστηρίου Ασθενών

Το Σύστημα Λογιστηρίου Ασθενών του ΟΠΣΝ διασυνδέεται με το βασικό Σύστημα Λογιστηρίου του Διοικητικού-οικονομικού Συστήματος. Διαχειρίζεται τις χρεώσεις των υπηρεσιών υγείας που δέχεται ο ασθενής στο νοσοκομείο υποστηρίζοντας την διαδικασία **χρέωσης**, (**τιμολόγησης**), των εξωτερικών και εσωτερικών ασθενών και των ταμείων τους καθώς και της **εκκαθάρισης των λογαριασμών ασθενών.**

Η **τιμολόγηση** ασθενών αφορά την διαδικασία καταγραφής και αποθήκευσης των δεδομένων για τον **υπολογισμό** του λογαριασμού ενός εξωτερικού ή εσωτερικού ασθενή για τις παρεχόμενες υπηρεσίες και περιλαμβάνει την χρέωση των ασθενών ή/ και των ασφαλιστικών τους ταμείων. Τα δεδομένα αυτά αφορούν τις ενέργειες που έγιναν στον ασθενή κατά την διάρκεια της παροχής υπηρεσιών υγείας και αφορούν το ημερήσιο νοσήλιο, τις εργαστηριακές εξετάσεις, τις ιατρικές πράξεις όπως επεμβάσεις κλπ, τα φάρμακα και τα υπόλοιπα υλικά.

Η **εκκαθάριση των λογαριασμών** ασθενών αφορά την διαδικασία παρακολούθησης των λογαριασμών των ασφαλιστικών οργανισμών, την έκδοση καταστάσεων εκκαθάρισης προς τα ταμεία με δεδομένα της τιμολόγησης των ασθενών κλπ.

Η διαδικασία τιμολόγησης των ιατρο-νοσηλευτικών υπηρεσιών είναι **αυτοματοποιημένη**, καθώς μέσω της επικοινωνίας του Ιατρονοσηλευτικού Υποσυστήματος με το Σύστημα Λογιστηρίου Ασθενών, υπολογίζονται αυτόματα οι χρεώσεις του ασθενή αναλόγως με τις ιατρικές πράξεις που πραγματοποιήθηκαν, το φαρμακευτικό και λοιπό υγειονομικό υλικό που αναλώθηκε κατά τη νοσηλεία του στο τμήμα / κλινική ή στα εξωτερικά ιατρεία, τις εργαστηριακές εξετάσεις που διενεργήθηκαν, κλπ..

Τέλος, στο Λογιστήριο Ασθενών δημιουργούνται όλες οι αποδείξεις παροχής υπηρεσιών προς απόδοση στον Ασθενή, ενώ υπολογίζονται αυτομάτως η συμμετοχή του Ασθενή και το ποσό που καλύπτεται από δημόσια ταμεία ή / και ασφαλιστικούς φορείς προς είσπραξη από το Νοσοκομείο. Οι υπάλληλοι του λογιστηρίου χρησιμοποιούν την διαδικτυακή εφαρμογή Σύστημα Αντιστοίχησης Κωδικοποιήσεων (ΣΑΚ), για να αντιστοιχήσουν τα Κ.Ε.Ν. στις διαγνώσεις εξόδου και τις ιατρικές πράξεις των ασθενών.

Οι βασικές λειτουργικότητες του συστήματος είναι:

1. Αναζήτηση ασθενή στο τοπικό ευρετήριο ασθενών του Νοσοκομείου
2. Εμφάνιση ή ενημέρωση καρτέλας δημογραφικών του ασθενή
3. Καταγραφή νέας καρτέλας δημογραφικών (Καταχώρηση Νέου Πολίτη) στην περίπτωση που η αναζήτηση ασθενή δεν έχει κανένα αποτέλεσμα
4. Διαχείριση Ασφαλιστικών Φορέων του ασθενή με δυνατότητα δήλωσης σειράς προτεραιότητας ασφαλιστικού φορέα.
5. Εμφάνιση λίστας παλαιότερων τιμολογίων
6. Προβολή λίστας με τα παλαιότερα τιμολόγια που έχουν κοπεί για ένα συγκεκριμένο ασθενή.
7. Προβολή των αναλυτικών στοιχείων του κάθε τιμολογίου
8. Εμφάνιση λίστας εισαγωγών του ασθενή σε κλινικές (ή επαφών του με το Νοσοκομείο ως εξωτερικός ασθενή)
9. Προβολή των δεδομένων συγκεκριμένων εισαγωγής
10. Εμφάνιση λίστας εκκρεμών χρεώσεων του ασθενή
11. Πρόσβαση στα δεδομένα χρέωσης/τιμολογίου (ημερήσια νοσήλια, ημέρες νοσηλείας, φάρμακα, εργαστηριακές πράξεις, ιατρικές πράξεις, υλικά) που σχετίζονται με συγκεκριμένη νοσηλεία ή επαφή του ασθενή στα εξωτερικά ιατρεία και εργαστήρια του Νοσοκομείου.
12. Τροποποίηση των δεδομένων χρέωσης/τιμολογίου (αλλαγή των τιμών χρέωσης, της ποσότητας χρέωσης, της έκπτωσης, της συμμετοχής)
13. Καταγραφή νέων δεδομένων χρέωσης (για φάρμακα, εργαστηριακές πράξεις, ιατρικές πράξεις, υλικά) σε συγκεκριμένο τιμολόγιο
14. Επανυπολογισμός τιμολογίου, προεπισκόπηση και εκτύπωση τιμολογίου
15. Εξαγωγή στοιχείων τιμολογίου σε άλλες εφαρμογές (word, excel κλπ)
16. Ολοκλήρωση διαδικασίας διαχείρισης τιμολογίου
17. Παρουσίασης συγκεντρωτικής λίστας ασθενών που είναι έτοιμοι προς Χρέωση
18. Ταξινόμηση λίστας ασθενών προς χρέωση με οποιαδήποτε στήλη
19. Διαχείριση Νέας Υποβολής για εσωτερικούς ή εξωτερικούς ασθενείς:

20. Συλλογή (αυτόματα) όλων των τιμολογίων που αφορούν εσωτερικούς ασθενείς προκειμένου να δημιουργηθεί η σχετική κατάσταση υποβολής
21. Δημιουργία (αυτόματα) συγκεντρωτικής κατάστασης για υποβολή τιμολογίων που αφορούν εσωτερικούς ασθενείς και εκτύπωση συγκεντρωτικής κατάστασης
22. Δημιουργία (αυτόματα) αναλυτικής κατάστασης για υποβολή τιμολογίων που αφορούν εσωτερικούς ασθενείς και εκτύπωση αναλυτικής κατάστασης
23. Ολοκλήρωση υποβολής
24. Παρακολούθηση/Διαχείριση προηγούμενων υποβολών:
25. Προβολή λίστας προηγούμενων υποβολών ανά ασφαλιστικό ταμείο και κατάσταση υποβολής
26. Προβολή αντικειμένων συγκεκριμένης υποβολής
27. Ενημέρωση ποσού έγκρισης για τα αντικείμενα συγκεκριμένης υποβολής – Παρακολούθηση Πληρωμών – Επανυποβολές

Σύστημα Διαχείρισης Ραντεβού

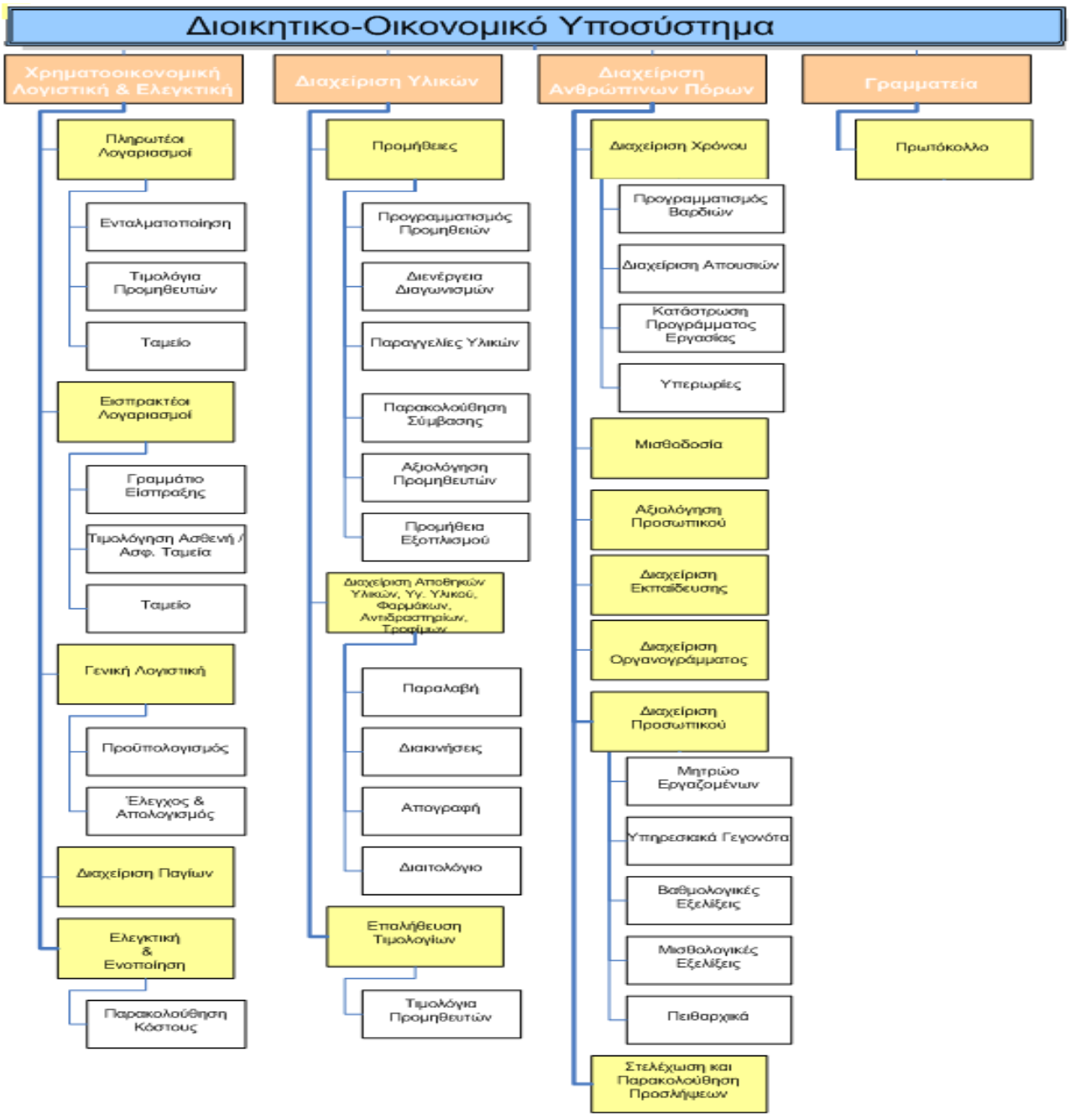
Το Σύστημα Διαχείρισης Ραντεβού υποστηρίζει την διαδικασία διαχείρισης ραντεβού για τη Γραμματεία Εξωτερικών και Απογευματινών Ιατρείων. Υλοποιείται από εξωτερικό συνεργάτη και το νοσοκομείο συνδέεται διαδικτυακά με αυτό. Οι ασθενείς μέσω του αριθμού 1535 κλείνουν το ραντεβού στο ιατρείο που επιθυμούν και υπάρχει δυνατότητα να κλειστεί ραντεβού από τη γραμματεία ΤΕΙ. Οι βασικές λειτουργικότητες του συστήματος είναι:

1. Διαχείριση ραντεβού
2. Επιλογή ιατρείου
3. Προβολή εβδομαδιαίου προγράμματος λειτουργίας ιατρείου
4. Προγραμματισμός νέου ραντεβού ή επαναλαμβανόμενου ραντεβού
5. Ακύρωση ραντεβού
6. Μεταφορά ραντεβού σε άλλο ιατρείο ή σε άλλη ημερομηνία/ώρα με βάση το ιατρείο
7. Χρέωση ραντεβού
8. Αναζήτηση/εύρεση πολίτη

9. Διαχείριση των δημογραφικών στοιχείων νέου πολίτη
10. Προβολή των δεδομένων σχετικά με τα ραντεβού ενός ασθενή (ιστορικό ραντεβού)
11. Τροποποίηση ραντεβού
12. Εκτυπώσεις

Διοικητικό – Οικονομικό Υποσύστημα

Στην εικόνα 2.5 απεικονίζεται το Διοικητικό – Οικονομικό Υποσύστημα του νοσοκομείου.



Εικόνα 2.5: Διοικητικό – Οικονομικό Υποσύστημα

Το Διοικητικό-Οικονομικό Υποσύστημα υλοποιείται με ενιαίο και ολοκληρωμένο τρόπο στην Κεντρική Υπηρεσία της ΥΠε και στα νοσοκομεία και περιλαμβάνει τα ακόλουθα υποσυστήματα:

1. Χρηματοοικονομική Λογιστική & Πάγια (Financial & Assets Accounting)
2. Ελεγκτική – Κοστολόγηση (Controlling)
3. Λογιστική Ενοποίηση (Legal Consolidation)
4. Διαχείριση Υλικών (Materials Management)
5. Διαχείριση Ανθρώπινων Πόρων (Human Resources)
6. Μισθοδοσία (Payroll)
7. Πρωτόκολλο

Το υποσύστημα της **Χρηματοοικονομικής Λογιστικής** απαρτίζεται από τις παρακάτω ενότητες :

Γενική Λογιστική: Είναι η βάση όλου του Διοικητικό-Οικονομικού συστήματος. Όλα τα υποσυστήματα επικοινωνούν και ενημερώνουν τη Λογιστική με στόχο την έγκαιρη άντληση οικονομικών πληροφοριών και αποτελεσμάτων.

Αναλυτική Λογιστική: Το κύκλωμα αυτό αποτελεί προέκταση του κυκλώματος της Γενικής Λογιστικής και σε συνδυασμό με την Ελεγκτική / Κοστολόγηση και τον ορισμό των κοστολογικών αντικειμένων παρέχει αναλυτική πληροφόρηση σχετικά με το κόστος ανά λειτουργία.

Εισπρακτέοι Λογαριασμοί: Τα βασικά δεδομένα των πελατών - ασθενών δημιουργούνται αυτόματα μέσω της εφαρμογής της διαχείρισης των ασθενών και είναι ίδια για όλες τις συνδεδεμένες μονάδες υγείας. Από τους εισπρακτέους λογαριασμούς παρακολουθούνται οι απαιτήσεις των πελατών-ασθενών του νοσοκομείου και των λοιπών συναλλασσόμενων όπως ασφαλιστικοί οργανισμοί.

Πληρωτέοι Λογαριασμοί: Το κύκλωμα των πληρωτέων λογαριασμών καλύπτει τη διαχείριση των συναλλακτικών σχέσεων του νοσοκομείου με τους προμηθευτές ειδών (υγειονομικά υλικά, φαρμακευτικά, ιατρικός εξοπλισμός κλπ) και υπηρεσιών. Οι πληρωτέοι λογαριασμοί συνδέονται άμεσα με την εφαρμογή της διαχείρισης των υλικών (προμηθειών και συμβάσεων).

Λογιστική Παγίων: Το υποσύστημα Διαχείρισης Παγίων επιτρέπει την παρακολούθηση του συνόλου των παγίων (πχ μηχανήματα και εξοπλισμός, κτήρια κλπ).

Οι διαδικασίες που σχετίζονται με την **Οικονομική Διαχείριση** είναι:

1. Κατάρτιση Προϋπολογισμού
2. Έλεγχος Προϋπολογισμού
3. Απολογισμός - Ισολογισμός
4. Παρακολούθηση Κόστους
5. Εισπράξεις / Επιχορηγήσεις
6. Διαχείριση Πληρωμών
7. Διαχείριση Παγίων
8. Ελεγκτική – Κοστολόγηση (Controlling)

Το συγκεκριμένο υποσύστημα καλύπτει τις διαδικασίες:

1. Κατάρτιση και έλεγχος Προϋπολογισμού
2. Παρακολούθηση κόστους
3. Ενοποίηση Οικονομικών Στοιχείων σε επίπεδο ΥΠΕ
4. Διαχείριση Υλικών (Materials Management)

Από το υποσύστημα **Διαχείρισης Υλικών** υλοποιούνται τα εξής:

1. Προμήθειες

   Στόχος της εφαρμογής των προμηθειών είναι η αυτοματοποίηση, η παρακολούθηση και ο έλεγχος των προμηθειών.

2. Διαχείριση Αποθηκών

   Η εφαρμογή των Αποθηκών διαχειρίζεται όλα τα είδη / υλικά που αγοράζονται από το νοσοκομείο και καλύπτει τις αποθήκες Υλικού, Φαρμακείου, Αντιδραστηρίων, Υγειονομικού Υλικού και Τροφίμων. Οι διαδικασίες που σχετίζονται με το υποσύστημα Διαχείρισης Υλικών είναι:

3. Προγραμματισμός Προμηθειών

    3.1. Διαγωνισμοί

    3.2. Συμβάσεις Αγορών, Συντήρησης, & Υπηρεσιών

    3.3. Παραγγελίες Υλικών & Υπηρεσιών

    3.4. Παρακολούθηση Συμβάσεων

    3.5. Τιμολόγια Προμηθευτών

    3.6. Παραλαβή Διακινήσεις

    3.7. Απογραφή

4. Διαιτολόγιο

Η **Διαχείριση Ανθρωπίνων Πόρων** αποτελεί το υποσύστημα με τις παρακάτω διαδικασίες που αφορούν στη Διαχείριση Προσωπικού.

1. Παρακολούθηση Προσλήψεων και Διορισμός προσωπικού
2. Παρακολούθηση Μετατάξεων
3. Μητρώο Προσωπικού
4. Εκπαίδευση Προσωπικού
5. Παρακολούθηση Μετατάξεων ανά κλάδο
6. Παρακολούθηση Πειθαρχικών παραπτωμάτων
7. Παρακολούθηση Αδειών
8. Κατάστρωση Προγράμματος Εργασίας Προσωπικού
9. Παρακολούθηση Αποχωρήσεων
10. Αξιολόγηση Προσωπικού
11. Παρακολούθηση Διοικητικών εξελίξεων
12. Παρακολούθηση Μισθολογικών εξελίξεων
13. Παρακολούθηση Υπερωριών Προσωπικού

Το υποσύστημα **Διαχείριση Μισθοδοσίας Προσωπικού** επιτρέπει την εκτέλεση των διαδικασιών για την προετοιμασία και έκδοση της μισθοδοσίας όλων των κατηγοριών προσωπικού καθώς και για την ενημέρωση όλων των εμπλεκόμενων φορέων. Αυτές είναι:

1. Προετοιμασία μισθοδοσίας
2. Έκδοση μισθοδοσίας
3. Αναδρομικές μισθοδοσίες
4. Υπολογισμός Δώρων και επιδόματος άδειας
5. Διασύνδεση με τράπεζες ή με το διατραπεζικό σύστημα ΔΙΑΣ
6. Διαδικασίες οριστικοποίησης μισθοδοσίας
7. Εκτυπώσεις
8. Αναλυτική Περιοδική Δήλωση ΙΚΑ

Πληροφοριακό Σύστημα Εργαστηρίων (Π.Σ.Ε.)

Αρχιτεκτονική του Π.Σ.Ε.

Το ΠΣΕ λειτουργεί ως ένα ολοκληρωμένο πληροφοριακό σύστημα αξιοποιώντας το πρωτόκολλο HL7 για την λειτουργική διασύνδεση των επιμέρους ΠΣΕ με το ΟΠΣΥ. Το σύστημα αποτελείται από τρεις «λογικές ενότητες»:

1. Μονάδα Επικοινωνίας με εξωτερικές εφαρμογές που διαχειρίζεται:
    1.1. Τα δημογραφικά στοιχεία του ασθενή και τα στοιχεία προέλευσης του όπως είναι η κλινική.
    1.2. Την παραγγελία των εξετάσεων του ασθενή μέσω του ΟΠΣΝ
    1.3. Την ενημέρωση του ιατρικού φακέλου του ΟΠΣΝ (επιστροφή εγκεκριμένων αποτελεσμάτων)
    1.4. Θεωρητικό υπολογισμό της ανάλωσης των αντιδραστηρίων των χρησιμοποιούμενων αναλυτών.
2. Μονάδα Επικοινωνίας με εργαστηριακά όργανα (αναλυτές)

Προσφέρει δύο βασικούς τρόπους επικοινωνίας με τα εργαστηριακά όργανα. Μέσω της σειριακής θύρας του υπολογιστή (και αντίστοιχα του αναλυτή) ή μέσω του πρωτοκόλλου TCP/IP εφ' όσον κάτι τέτοιο υποστηρίζεται από το όργανο. Και στις δύο περιπτώσεις η επικοινωνία αυτή μπορεί να είναι είτε μονόδρομη είτε αμφίδρομη, πράγμα το οποίο και πάλι εξαρτάται από τις δυνατότητες του οργάνου προς σύνδεση. Η μονάδα αυτή επικοινωνεί εσωτερικά με τον application server της εφαρμογής τόσο για τον προγραμματισμό εξετάσεων στον αναλυτή, την επιστροφή των αποτελεσμάτων αλλά και την διεξαγωγή του ποιοτικού ελέγχου.

3. Μονάδα Λογικής της Εφαρμογής (Application Server)

Αυτή η μονάδα έχει την ευθύνη επικοινωνίας με την Βάση Δεδομένων. Τα δύο υποσυστήματα που περιγράφηκαν παραπάνω, ουσιαστικά επικοινωνούν με τον application server ο οποίος αναλαμβάνει την περαιτέρω επικοινωνία με την database. Η «γνώση» που διαχειρίζεται το συγκεκριμένο υποσύστημα έχει να κάνει όλες ουσιαστικά τις έννοιες του εργαστηρίου όπως:

- Οργανωτική Δομή των Εργαστηρίων
- Διαχείριση Δειγμάτων
- Κύκλωμα Παραγγελίας και δημιουργίας Work lists
- Παραλαβή αποτελεσμάτων, έλεγχος, έγκριση αυτών
- Ποιοτικός Έλεγχος
- Αναφορές ενημέρωσης ιατρικού προσωπικού και διοίκησης

Οι διαδικασίες του ΠΣΕ είναι οι εξής:

Παραγγελία εξετάσεων: Η εισαγωγή – καταχώρηση της παραγγελίας γίνεται από αντίστοιχα τμήματα του Νοσοκομείου (Κλινικές, ΜΕΘ κλπ) αν πρόκειται για εσωτερικούς ασθενείς. Αν πρόκειται για εξωτερικούς ασθενείς γίνεται από τα εξωτερικά Ιατρεία.

Αρίθμηση δειγμάτων – λήψη δειγμάτων: Με την καταχώρηση της παραγγελίας των εξετάσεων προς τα εργαστήρια, το σύστημα αυτόματα ανιχνεύει το είδος, την ποσότητα, το εργαστήριο ή το τμήμα του εργαστηρίου που προορίζονται τα δείγματα, και αντιστοιχεί τα δείγματα με τον αριθμό (α/α δείγματος – specimen ID) του/των δείγματος/ων σύμφωνα με τους

κανόνες αρίθμησης δειγμάτων που έχουν καθορίσει τα εργαστήρια, οπότε τυπώνεται το παραπεμπτικό των εξετάσεων και οι αντίστοιχες ετικέτες γραμμωτού κώδικα (Bar Code) ανά δείγμα. Η εκτύπωση ετικετών γίνεται σε προεπιλεγμένα σημεία. Τυπώνονται είτε στο σημείο αιμοληψίας των κλινικών είτε στο σημείο καταχώρησης-δημιουργίας του ηλεκτρονικού παραπεμπτικού, εφόσον οι λήψεις γίνεται από προσωπικό της κάθε κλινικής, είτε στα εργαστήριο αν χρησιμοποιείται προσωπικό των εργαστηρίων για τις λήψεις των δειγμάτων. Όλη η παραπάνω διαδικασία γίνεται πλήρως αυτοματοποιημένα.

Παραλαβή δειγμάτων: Η παραλαβή των δειγμάτων (το καθένα σημειωμένο με την ειδική ετικέτα του) ανά εργαστήριο, γίνεται στον ειδικό χώρο παραλαβής – διαλογής των δειγμάτων και στην συνέχεια γίνεται η προετοιμασία των δειγμάτων και η προώθησή τους στους αντίστοιχους χειριστές αναλυτών ή στο κατάλληλο προσωπικό. Μετά την καταχώρηση της παραγγελίας τα διάφορα εργαστήρια μπορούν αυτόματα να πάρουν το μέρος εκείνο της παραγγελίας (βάσει των εξετάσεων και της ευθύνης του κάθε τμήματος αναλυτή η χειριστή) και να το διεκπεραιώσουν.

Διενέργεια εξετάσεων – αναλύσεων: Τα δείγματα κατηγοριοποιούνται βάσει τη προτεραιότητας εκτέλεσης τους έτσι ώστε αναλύσεις που πρέπει να επεξεργαστούν αμέσως (Μ.Ε.Θ., Χειρουργεία, κλπ) να δώσουν αποτελέσματα στο μικρότερο δυνατό χρόνο. Έτσι προωθούνται για ανάλυση μόνο οι παραγγελίες των οποίων τα δείγματα έχουν φτάσει στο εργαστήριο. Αν οι αναλυτικές συσκευές το επιτρέπουν (ανάγνωση barcodes), τότε τα δείγματα τοποθετούνται στον αναλυτή, αυτός διαβάζει τον κωδικό barcode του δείγματος και ζητά από το σύστημα τη λίστα των προς εκτέλεση εξετάσεων.

Πριν τυπωθούν ή αποσταλούν τα απαντητικά, αρμόδιο πρόσωπο του εργαστηρίου (π.χ. Ο διευθυντής του) εγκρίνει τα τελικά αποτελέσματα ή ζητά νέες αναλύσεις προκειμένου να εκφέρει τη τελική του άποψη. Η διαδικασία έγκρισης διενεργείται ηλεκτρονικά μέσω του πληροφοριακού συστήματος εργαστηρίων.

Αποστολή/εκτύπωση αποτελεσμάτων: Στο τελικό στάδιο τα αποτελέσματα εκτυπώνονται και υπογράφονται αν αποστέλλονται γραπτώς ή αποστέλλονται ηλεκτρονικώς στους ενδιαφερόμενους. Έτσι τα αποτελέσματα καταλήγουν στους τελικούς αποδέκτες (κλινικές, θεράποντες ιατροί, ΜΕΘ, εξωτερικά ιατρεία, κλπ) και διαβάζονται είτε σε έντυπη μορφή είτε μέσω οθόνης υπολογιστή στις κλινικές.

Στατιστικές – πληροφόρηση προς τη διοίκηση: Επίσης υπάρχει και μια σειρά από άλλες διαδικασίες που εκτελούν τα εργαστήρια όπως:

- Ποιοτικός έλεγχος αναλυτικών συσκευών
- Αναφορές και στατιστική επεξεργασία δεδομένων για ιατρικό προσωπικό
- Αναφορές και στατιστική επεξεργασία δεδομένων για τη διοίκηση

Υποσύστημα Επιχειρηματικής Ευφυΐας (BI)

Για την κάλυψη των αναγκών της Υ.Π.Ε. και του νοσοκομείου υπάρχει λογισμικό Επιχειρηματικής Ευφυΐας (Business Intelligence – BI). Οι έγκαιρες και αξιόπιστες πληροφορίες μπορούν να βοηθήσουν στην καλύτερη αντίληψη του επιχειρηματικού σκηνικού, να υποστηρίξουν τις αποφάσεις και να βελτιώσουν τα αποτελέσματα της υπηρεσίας. Μερικές από τις αναλύσεις οι οποίες τις οποίες μπορεί να κάνει είναι οι εξής:

Ανάλυση κίνησης ασθενών: Εισαγωγές και εξαγωγές ασθενών, διάστημα εναλλαγής ασθενών, μέση διάρκεια νοσηλείας, φόρτος νοσοκομείου κλπ.

Οικονομικά στοιχεία: Μέσο κόστος νοσηλείας, φαρμάκων, διαγνωστικών εξετάσεων, χειρουργικών επεμβάσεων κλπ.

Ανθρώπινοι πόροι: Πληρότητα προσωπικού, μεταβολές προσωπικού, παραγωγικότητα, κλπ.

Άντληση και Ανάλυση Δεδομένων: Το BI συνεργάζεται με πολλά εξωτερικά συστήματα και συνδέεται με τις βάσεις δεδομένων όλων των συστημάτων. Το προτεινόμενο σύστημα περιλαμβάνει εξελιγμένες δυνατότητες ανάλυσης.

Ad hoc queries- Εργαλεία δημιουργίας αναφορών: Το BI έχει την δυνατότητα δημιουργίας αναζητήσεων κατά περίπτωση (ad hoc queries) με γραφικό τρόπο. Επιπλέον διαθέτει εργαλεία δημιουργίας απλών αναφορών (wizards) για τη διευκόλυνση του τελικού χρήστη.

Ανωνυμία Δεδομένων: Όπου απαιτείται η αλλοίωση των στοιχείων για τήρηση ανωνυμίας, προγραμματίζεται η μετατροπή των εισερχόμενων στοιχείων.

Σύστημα Μονάδων Πρωτοβάθμιας Φροντίδας Υγείας - ΠΦΥ

Στο «HOSPITAL» ανήκουν διοικητικά δύο Περιφερειακά Ιατρεία - Π.Ι.

Ηλεκτρονική συνταγογράφηση – παραγγελία εξετάσεων

Στο νοσοκομείο και στα Π.Ι. οι γιατροί χρησιμοποιούν υποχρεωτικά την εφαρμογή της Η.Δ.Ι.Κ.Α για την ηλεκτρονική συνταγογράφηση και ηλεκτρονική παραγγελία εξετάσεων.

Κεφάλαιο 3
Ασφάλεια του ΟΠΣΥ

Η ασφάλεια των Πληροφοριακών Συστημάτων – Π.Σ. είναι ζήτημα κρίσιμης σημασίας στη σύγχρονη κοινωνία. Οργανισμοί, επιχειρήσεις, δημόσιες υπηρεσίες βασίζονται για την εκτέλεση και αποδοτικότητα της εργασίας τους σε αυτά.

3.1 Ασφάλεια Πληροφορικού Συστήματος

Κάθε δυσλειτουργία του Π.Σ. προκαλεί πρόβλημα στην ομαλή διενέργεια της εργασίας αυτής. Ανάλογα με το πεδίο εργασιών, οι επιπτώσεις μπορεί να είναι οικονομικές απώλειες έως και απειλή της ανθρώπινης ζωής αν αφορούν στρατιωτικά συστήματα, συστήματα ελέγχου εναέριας κυκλοφορίας, νοσοκομεία. Οι απειλές που αντιμετωπίζει ένα Π.Σ. χωρίζονται σε δύο κατηγορίες:

1. Απειλές από κακόβουλες ενέργειες
2. Απειλές από ακούσιες ενέργειες

Στις απειλές περιλαμβάνονται μεταξύ των άλλων:

1. Εισαγωγή κακόβουλου κώδικα και ιομορφικού λογισμικού
2. Μη εξουσιοδοτημένη χρήση εφαρμογών
3. Πλαστή χρήση ταυτότητας νόμιμου χρήστη
4. Κατάχρηση πόρων
5. Παρακολούθηση επικοινωνιών
6. Κλοπή πληροφοριών
7. Κλοπή υλικού
8. Σφάλματα χειρισμού και συντήρησης
9. Τεχνική αστοχία συστήματος
10. Αστοχία λογισμικού
11. Δολιοφθορά και εγκλήματα ειδικής βίας
12. Απώλεια παροχής ηλεκτρικής ενέργειας
13. Φυσικές καταστροφές (φωτιά, πλημμύρα κλπ)
14. Βλάβη στα κλιματιστικά

Τα κρούσματα παραβίασης της ασφάλειας Π.Σ., είτε γίνονται με σκοπό το κέρδος, είτε με σκοπό την προσωπική ευχαρίστηση των δραστών είτε ακόμη σχετίζονται με κοινωνικό – πολιτικό ακτιβισμό, είναι στην εποχή μας πολύ συχνά και σε ποικίλες μορφές.

Όσον αφορά το ΟΠΣΥ, ένα μεγάλο μέρος των πληροφοριών που διαχειρίζεται εμπίπτουν στο Ιατρικό Απόρρητο ή αποτελούν Ευαίσθητα Προσωπικά Δεδομένα, τα οποία είναι εμπιστευτικά και δεν πρέπει να αποκαλύπτονται. Επίσης τα δεδομένα που αφορούν στη παροχή υπηρεσιών υγείας και κατά συνέπεια στη ζωή του ασθενή, είναι προφανές ότι πρέπει να είναι αξιόπιστα, η τροποποίησή τους να είναι ελεγχόμενη και να είναι διαθέσιμα όταν αυτό είναι απαραίτητο.

Ανησυχητικό είναι το γεγονός ότι από το 2009 μέχρι τις αρχές του 2012 στην Αμερική περισσότερες από 18.000.000 ιατρικές πληροφορίες ασθενών τέθηκαν σε κίνδυνο ενώ οι παραβιάσεις σε ιατρικούς τομείς αυξήθηκαν κατά 32%. [13]

Σύμφωνα με τον μη κερδοσκοπικό οργανισμό Word Privacy Forum [14] η αξία στην παράνομη αγορά για την κλεμμένη ιατρική πληροφορία είναι 50$ ενώ είναι 1$ για κλεμμένο αριθμό κοινωνικής ασφάλισης. Αντίστοιχα η αξία κλεμμένης ιατρικής ταυτότητας είναι 20.000 $ ενώ απλής ταυτότητας 2.000$.

Στο Αμερικανικό Τμήμα Υγείας και Εξυπηρέτησης Πολιτών (Department of Health and Human Services - HHS), αναφέρονται και μετά ανακοινώνονται, παραβιάσεις ασφάλειας οι οποίες αφορούν σε περιπτώσεις που η παραβίαση επηρεάζει 500 ή περισσότερους πολίτες. Μερικά από αυτά είναι [15]:

University Health System

State: Nevada

Approx. # of Individuals Affected: 7,526

Date of Breach: 6/11/10

Type of Breach: Theft

Location of Breached Information: Network Server

Children's Hospital & Research Center at Oakland

State: California

Approx. # of Individuals Affected: 1,000

Date of Breach: 5/25/10 and 5/26/2010

Type of Breach: Other

Location of Breached Information: Paper

Sinai Hospital of Baltimore, Inc.

State: Maryland

Business Associate Involved: Aramark Healthcare Support Services, Inc.

Approx. # of Individuals Affected: 937

Date of Breach: 5/03/10

Type of Breach: Other

Location of Breached Information: E-mail

The Children's Medical Center of Dayton

State: Ohio

Approx. # of Individuals Affected: 1,001

Date of Breach: 4/22/10

Type of Breach: Other

Location of Breached Information: E-mail

Άλλα περιστατικά που έχουν συμβεί στις ΗΠΑ είναι και τα παρακάτω:

Hackers παραβίασαν τους Servers ιατρικών κέντρων και νοσοκομείων και κρυπτογράφησαν τα δεδομένα ζητώντας λύτρα για να τα αποκρυπτογραφήσουν.[16]

Την ίδια περίοδο το Utah Health Department ανακοίνωσε κλοπή των ιατρικών δεδομένων σε 280.000 πολίτες της Utah. [17]

Αλλά και στην Ελλάδα έχουμε παρόμοια περιστατικά παραβίασης ασφάλειας σε δημόσιους οργανισμούς και υγειονομικούς οργανισμούς οι οποίες έχουν δημοσιευθεί ή ανακοινωθεί.

Σε εξέλιξη βρίσκεται από τη Δίωξη Ηλεκτρονικού Εγκλήματος, η διερεύνηση της ψηφιακής επίθεσης στην ιστοσελίδα του υπουργείου Δικαιοσύνης. Διερευνώνται τα ηλεκτρονικά ίχνη των επιτιθέμενων. Υπενθυμίζεται ότι οι χάκερς ανέφεραν σε βίντεο ότι «η δικαιοσύνη γεννήθηκε στην χώρα σας και εσείς την σκοτώσατε». Προειδοποιούν ότι θα παραβιάσουν και άλλες ιστοσελίδες υπουργείων, και Ελληνικών Μέσων Ενημέρωσης. [18]

«Στο μικροσκόπιο των Δικαστικών Αρχών μπαίνει το υπουργείο Οικονομικών και οι υπηρεσίες του που έχουν άμεση σχέση με την καταγραφή οικονομικών και προσωπικών δεδομένων μετά την ολοκλήρωση της επιχείρησης της Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας και την σύλληψη των υπευθύνων εταιρείας πληροφορικής και επεξεργασίας στοιχείων στη Δάφνη. Η συγκεκριμένη υπόθεση θεωρείται από τα στελέχη των Διωκτικών Αρχών ως η «κορυφή του παγόβουνου», καθώς σύμφωνα με τα πρώτα στοιχεία από υπηρεσίες του υπουργείου Οικονομικών διοχετεύθηκαν στην αγορά εκατομμύρια αρχεία προσωπικών, οικονομικών και φορολογικών δεδομένων με στοιχεία που περιέχουν φορολογικές δηλώσεις, οφειλές πολιτών, στοιχεία του «Τειρεσία», στοιχεία για περιουσιακά ακόμη και τις δόσεις που χρωστούν στις εφορίες και στοιχεία συναλλαγών τους με το δημόσιο.» [19]

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα επέβαλε σε ασφαλιστική εταιρεία πρόστιμο 10.000 ευρώ για παράνομη συλλογή ευαίσθητων προσωπικών δεδομένων ασφαλισμένης της και ισόποσο πρόστιμο σε ιδιωτικό θεραπευτήριο για παράνομη διαβίβαση ιατρικού φακέλου στην ασφαλιστική εταιρεία χωρίς να ενημερώσει την ενδιαφερόμενη ασφαλισμένη και την Αρχή. Το ιδιωτικό θεραπευτήριο διαβίβασε στην ασφαλιστική εταιρεία όλο τον ιατρικό φάκελο της ασφαλισμένης και όχι μόνον τα στοιχεία που ήταν αναγκαία και απαραίτητα για τη συγκεκριμένη ασφαλιστική περίπτωση, χωρίς την προηγούμενη ενημέρωση της ασφαλισμένης για τη διαβίβαση αυτή. Έτσι, η Αρχή έκρινε ότι η ασφαλιστική συνέλεξε, καταχώρισε στο αρχείο της και επεξεργάσθηκε περαιτέρω τα ευαίσθητα δεδομένα υγείας της ασφαλισμένης, με τη διαβίβαση του ιατρικού φακέλου της από το ιδιωτικό θεραπευτήριο, χωρίς την προηγούμενη ενημέρωση και συγκατάθεση της ενδιαφερομένης, κατά παράβαση των διατάξεων των άρθρων 5 και 11 παρ. 1 του Ν. 2472/1997. [20]

Γίνεται λοιπόν απολύτως αναγκαία η λήψη των κατάλληλων μέτρων για την προστασία του ΟΠΣΥ και του ΟΠΣΝ από παραβιάσεις ασφάλειας.

3.1.1 Τι Ονομάζουμε Ασφάλεια ΠΣ;

Ασφάλεια Πληροφοριακού Συστήματος (Information System Security) είναι [02] η ασφάλεια πληροφοριών και υπολογιστικού συστήματος για το δεδομένο πληροφοριακό σύστημα, όπου:

Ασφάλεια Υπολογιστικού Συστήματος (IT System Security) είναι η διασφάλιση διαθεσιμότητας συστήματος και ασφάλειας πληροφοριών καθώς και των παραμέτρων που αποτελούν τμήμα του Υπολογιστικού Συστήματος.

Διαθεσιμότητα Συστήματος (System Availability) είναι η αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης υπολογιστικών πόρων σε εξουσιοδοτημένους χρήστες.

Ασφάλεια Πληροφοριών(Information Security) είναι η διασφάλιση εμπιστευτικότητας, ακεραιότητας, αυθεντικότητας, εγκυρότητας, και διαθεσιμότητας πληροφοριών.

Εμπιστευτικότητα (Confidentiality) είναι η αποφυγή αποκάλυψης πληροφοριών χωρίς την άδεια του ιδιοκτήτη τους

Ακεραιότητα (Integrity) είναι η αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας.

Αυθεντικότητα (Authenticity) είναι η αποφυγή ατελειών και ανακριβειών κατά τη διάρκεια εξουσιοδοτημένων τροποποιήσεων μιας πληροφορίας.

Εγκυρότητα (Validity) είναι η απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας.

Διαθεσιμότητα πληροφοριών (Information Availability) είναι η αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας σε εξουσιοδοτημένους χρήστες.

Υπηρεσία είναι ένα σύνολο από λειτουργίες που παρέχει ένα Υπολογιστικό Σύστημα σε ένα Χρήστη.

Η ασφάλεια ενός πληροφοριακού συστήματος παρουσιάζει ιδιαιτερότητες και δυσκολίες ως επιστημονικός ερευνητικός χώρος αλλά και ως επιστημονική πρακτική [03]. Ειδικότερα η ασφάλεια και η προστασία του ΟΠΣΥ, το οποίο είναι ένα πολύπλοκο και ετερογενές σύστημα δεν

είναι καθόλου απλή υπόθεση. Το ΟΠΣΥ θα πρέπει να προστατεύεται από τις κάθε μορφής απειλές, χωρίς όμως, ταυτόχρονα, η προστασία αυτή να εμποδίζει την ροή των πληροφοριών. Μερικές από τις δυσκολίες που παρουσιάζονται στην ενσωμάτωση ενός συστήματος ασφάλειας σε ένα Π.Σ. είναι οι εξής:

Δυσκολία επικοινωνίας των επαγγελματιών της πληροφορικής με τις διοικήσεις των οργανισμών όσον αφορά την κατανόηση από τις διοικήσεις της αναγκαιότητας κατανάλωσης πόρων – σε χρήμα, προσωπικό κλπ – για την ασφάλεια των συστημάτων.

Η δυσκολία εμπέδωσης των χρηστών των Π.Σ. της ανάγκης για ασφάλεια ώστε να εμπλακούν ενεργητικά σε αυτή.

Η δυσκολία ανάπτυξης ενός ολοκληρωμένου, αποδοτικού και αποτελεσματικού σχεδίου ασφάλειας.

Για την επίλυση των παραπάνω προβλημάτων και την βέλτιστη αντιμετώπιση των προβλημάτων ασφάλειας, τις δύο τελευταίες δεκαετίες έχουν αναπτυχθεί **πρότυπα** και **μεθοδολογίες** για την ανάπτυξη και εφαρμογή τεχνικών ασφάλειας σε ένα πληροφοριακό σύστημα.

ΠΡΟΤΥΠΑ

Ένα διαδεδομένο πρότυπο που αφορά στην ασφάλεια πληροφοριακών συστημάτων είναι το ISO/IEC 27000. Η σειρά των προτύπων αυτών περιλαμβάνει τα πρότυπα ασφάλειας πληροφοριών που εκδίδονται από τον Διεθνή Οργανισμό Τυποποίησης (International Organization for Standardization - ISO) και την Διεθνή Ηλεκτροτεχνική Επιτροπή (International Electrotechnical Commission –IEC). Ένα μέρος των προτύπων που περιλαμβάνει είναι [21]:

ISO/IEC 27000:2012: Είναι μια επισκόπηση του πρότυπου και ένα λεξικό των χρησιμοποιούμενων όρων

ISO/IEC 27001:2005: Ορίζει τις προδιαγραφές για τον κύκλο ζωής (εγκατάσταση, εφαρμογή, λειτουργία, παρακολούθηση, αναθεώρηση και βελτίωση) ενός τεκμηριωμένου Συστήματος Διαχείρισης Ασφάλειας των Πληροφοριών (Information Security Management System - ISMS) σε ένα οργανισμό. Είναι σχεδιασμένο να υποστηρίζει την επιλογή των καταλληλότερων μέτρων και

ελέγχων σε σχέση με το είδος του οργανισμού και το είδος των κινδύνων που απειλούν την ασφάλειά του.

ISO/IEC 27002:2005: Καθορίζει τις οδηγίες και τις γενικές αρχές που πρέπει να εφαρμοστούν στον κύκλο ζωής ενός ISMS. Οι στόχοι και οι έλεγχοι που ορίζει το πρότυπο συμμορφώνονται με τις απαιτήσεις που έχουν οριστεί από την ανάλυση κινδύνων του οργανισμού. Αναφέρεται στα παρακάτω πεδία:

1. Πολιτική ασφάλειας
2. Οργάνωση της ασφάλειας της πληροφορίας
3. Διαχείριση των αγαθών
4. Ασφάλεια ανθρώπινου δυναμικού
5. Φυσική ασφάλεια και ασφάλεια περιβάλλοντος
6. Διαχείριση επικοινωνιών και λειτουργιών
7. Έλεγχοι πρόσβασης
8. Κτήση, ανάπτυξη και συντήρηση πληροφοριακού συστήματος
9. Διαχείριση περιστατικού παραβίασης της ασφάλειας
10. Διαχείριση επιχειρηματικής συνέχειας
11. Συμμόρφωση με τις οδηγίες

ISO/IEC 27003:2010: Περιέχει οδηγίες και βοήθεια για την ανάπτυξη και εφαρμογή του ISMS σύμφωνα με το ISO/IEC 27001:2005.

ISO/IEC 27004:2009: Περιέχει οδηγίες για την ανάπτυξη και χρήση των μέτρων και των μετρήσεων για την ασφάλεια των πληροφοριών, με σκοπό την αποτελεσματικότητα ενός ISMS, όπως αυτό έχει οριστεί από το ISO/IEC 27001:2005.

ISO/IEC 27005:2011: Περιέχει υποστηρικτικές οδηγίες για την εφαρμογή ενός ISMS.

ISO/IEC 27006:2011: Καθορίζει τις απαιτήσεις και παρέχει καθοδήγηση για την απόκτηση ISMS πιστοποίησης.

ΜΕΘΟΔΟΛΟΓΙΑ

Η πλέον διαδομένη μεθοδολογία, για την προστασία της ασφάλειας ενός πληροφοριακού συστήματος είναι η **μεθοδολογία της ανάλυσης και διαχείρισης επικινδυνότητας**.

Η ανάλυση επικινδυνότητας απαντά στο ερώτημα επιλογής αντιμέτρων που θα προσφέρουν προστασία ανάλογη των κινδύνων που απειλούν το ΠΣ. Εδώ η επικινδυνότητα εκτιμάται ως συνάρτηση της πιθανότητας εμφάνισης μίας απειλής και της σχετικής ευπάθειας του συστήματος που επιτρέπει στην απειλή να πραγματοποιηθεί. Αντίστοιχα, το κόστος από την πραγματοποίηση ενός επεισοδίου εκτιμάται με βάση την επίπτωση πάνω στον οργανισμό, που θα έχει η ζημιά που θα προκληθεί στα αγαθά του ΠΣ. Έτσι, η επικινδυνότητα εκτιμάται ως συνάρτηση τριών παραγόντων:

1. Της αξίας των αγαθών (assets), που προκύπτει από την αντίστοιχη επίπτωση της ζημιάς που θα υποστούν,
2. Της σοβαρότητας των απειλών (threats) και
3. Του επιπέδου της ευπάθειας (vulnerability) του ΠΣ.

Οι τεχνικές ανάλυσης της επικινδυνότητας χωρίζονται σε δύο κατηγορίες. Η πρώτη κατηγορία είναι η **ποσοτική (quantitative)** ανάλυση. Στην ανάλυση αυτή γίνεται προσπάθεια προσδιορισμού αριθμητικών τιμών για τις παραμέτρους της ανάλυσης. Π.χ. υπολογισμός χρηματικής αξίας αγαθών και κόστους απωλειών, κόστος αντίμετρων κλπ. Αυτή η προσέγγιση εξετάζει δύο ζητήματα [22]:

α) τη πιθανότητα ενός γεγονότος να συμβεί και

β) τη πιθανή απώλεια που μπορεί να επέλθει .

Μια ενιαία εικόνα παράγεται από αυτά τα δύο στοιχεία, απλά πολλαπλασιάζοντας τις πιθανές ζημιές (μετρούμενη σε νομισματικούς όρους) από την πιθανότητα της (που μετράται ως ποσοστό). Αυτό ονομάζεται μερικές φορές ετήσια προσδόκιμη απώλεια ή το εκτιμώμενο ετήσιο κόστος. Όσο υψηλότερος είναι ο βαθμός που παράγεται για ένα γεγονός, τόσο πιο σοβαρό είναι για το ΠΣ. Η ποσοτική ανάλυση εγκαταλείφθηκε λόγω δυσκολίας εφαρμογής της. Η δεύτερη κατηγορία και η πιο διαδεδομένη σήμερα, είναι η **ποιοτική (qualitative)** ανάλυση και είναι η προσέγγιση που αναμένεται από τη παράγραφο 4.2.1.d (Identify the risks) του προτύπου

ISO/IEC 27001. Στην ποιοτική ανάλυση δεν δίνονται ακριβείς αριθμητικές τιμές. Χρησιμοποιούνται τιμές από προαποφασισμένες κλίμακες. Οι τιμές μπορεί δηλαδή να είναι, χαμηλό, μέτριο, μεγάλο ή η κλίμακα 1 έως 10 κλπ. Αριθμητικά στοιχεία πιθανότητας δεν είναι απαραίτητα, και μόνο η πιθανή απώλεια χρησιμοποιείται. Οι περισσότερες ποιοτικές μεθοδολογίες ανάλυσης κινδύνου χρησιμοποιούν μια σειρά από αλληλένδετα στοιχεία που καταγράφονται σε μορφή πίνακα σε μια φόρμα ή φύλλο εργασίας. Έτσι για κάθε αγαθό του ΠΣ εντοπίζονται ο ιδιοκτήτης, οι απειλές, τα τρωτά σημεία του και οι επιπτώσεις. Με αυτή την ανάλυση αποφεύγονται πολύπλοκοι υπολογισμοί με αποτέλεσμα να χρειάζεται λιγότερο χρόνο και πόρους σε σχέση με την ποσοτική.

Η ανάλυση της επικινδυνότητας αποτελεί προϋπόθεση για την μετέπειτα διαχείριση της, που είναι και ο αντικειμενικός στόχος της όλης προσπάθειας. Ο όρος διαχείριση επικινδυνότητας αναφέρεται στον έλεγχο της επικινδυνότητας ώστε να παραμένει σε αποδεκτά επίπεδα. Η επικινδυνότητα μπορεί να μειωθεί, με την εφαρμογή αντιμέτρων, να μεταβιβαστεί, π.χ. με ασφάλιση, ή να αναληφθεί, δηλαδή να αποδεχθούμε ότι είμαστε διατεθειμένοι να υποστούμε τις επιπτώσεις αν συμβεί ένα επεισόδιο.

Η μεθοδολογία δεν περιγράφει συγκεκριμένες μεθόδους για την ανάλυση και αποτίμηση της επικινδυνότητας. Προσδιορίζει, όμως, ορισμένα στάδια που θα πρέπει να ακολουθηθούν. Σύμφωνα με το Διεθνή Οργανισμό Τυποποίησης (ISO – International Organization for Standardization) τα στάδια αυτά είναι:

1. Προσδιορισμός και αποτίμηση των αγαθών (assets).
2. Εκτίμηση της απειλής.
3. Εκτίμηση της ευπάθειας.
4. Εκτίμηση των υφισταμένων μέσων προστασίας.
5. Υπολογισμός της επικινδυνότητας.

Τα στάδια που περιγράφει ο ISO αποτελούν ένα γενικό πλαίσιο. Μπορούν να εξειδικευθούν, να συγχωνευθούν, να αντιστραφεί η σειρά τους κ.λπ., όμως κάθε μέθοδος ανάλυσης επικινδυνότητας θα πρέπει να τα συμπεριλάβει σε κάποια μορφή.

Με τον υπολογισμό της επικινδυνότητας ολοκληρώνεται η ανάλυση επικινδυνότητας. Το ζητούμενο, όμως είναι ο περιορισμός της επικινδυνότητας εντός αποδεκτών ορίων. Αυτό είναι το

αντικείμενο της διαχείρισης επικινδυνότητας. Η διαχείριση της επικινδυνότητας περιλαμβάνει τα εξής στάδια:

1. Επιλογή αντιμέτρων (countermeasures, safeguards).
2. Καθορισμός πολιτικής ασφάλειας.
3. Σύνταξη σχεδίου ασφάλειας.
4. Εφαρμογή και παρακολούθηση σχεδίου ασφάλειας.

Το Σχέδιο Ασφάλειας αποτελεί το βασικό εργαλείο για τη διαχείριση της επικινδυνότητας και περιλαμβάνει:

α) την πολιτική ασφάλειας,

β) τα αντίμετρα και

γ) τη στρατηγική εφαρμογής του σχεδίου.

Στα πλεονεκτήματα της ανάλυσης και διαχείρισης επικινδυνότητας περιλαμβάνονται τα παρακάτω:

Δίνει τη δυνατότητα αιτιολόγησης του κόστους των αντιμέτρων.

Αποτελεί ένα εργαλείο επικοινωνίας ανάμεσα στους ειδικούς των ΠΣ και τη διοίκηση των οργανισμών, καθώς επιτρέπει την έκφραση του προβλήματος της ασφάλειας σε γλώσσα κατανοητή από τη διοίκηση, αντιμετωπίζοντας την ασφάλεια ως επένδυση που αποτιμάται με όρους κόστους/οφέλους.

Είναι αρκετά ευέλικτη, ώστε να μπορεί να ενταχθεί σε διάφορα επιστημονικά πλαίσια και να εφαρμόζεται είτε αυτούσια, είτε σε συνδυασμό με άλλες μεθοδολογίες.

Καλύπτει τις απαιτήσεις της ευρωπαϊκής και ελληνικής νομοθεσίας, που απαιτούν από τα ΠΣ, τα οποία επεξεργάζονται προσωπικά δεδομένα, τη λήψη μέτρων προστασίας, έτσι ώστε "να εξασφαλίζεται επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων" (Νόμος 2472/1997, άρθρο 10, παρ. 3).

Διευκολύνει την καλύτερη κατανόηση της φύσης και της λειτουργίας του πληροφοριακού συστήματος. Αποτελεί, δηλαδή, ένα μέσο τεκμηρίωσης και ανάλυσης του πληροφοριακού συστήματος.

Αποτελεί την πλέον διαδεδομένη μεθοδολογία σχεδιασμού και διαχείρισης της ασφάλειας ΠΣ και έχει εφαρμοστεί με επιτυχία σε ένα μεγάλο πλήθος περιπτώσεων.

Παράλληλα όμως, η μεθοδολογία αυτή εμπεριέχει σημαντική υποκειμενικότητα στις εκτιμήσεις τόσο της αξίας των αγαθών όσο και στην αποτίμηση απειλών και ευπάθειας. Η υποκειμενικότητα αυτή συχνά συγκαλύπτεται πίσω από την συστηματικότητα των περισσότερων μεθόδων ανάλυσης επικινδυνότητας και την αντικειμενικότητα των εργαλείων που υποστηρίζουν τις σχετικές μεθόδους.

Μερικές από τις σημαντικότερες μεθόδους ανάλυσης και διαχείρισης επικινδυνότητας είναι οι εξής:

- Security By Analysis (SBA)
- MARION
- CCTA Risk Analysis and Management Method (CRAMM)
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

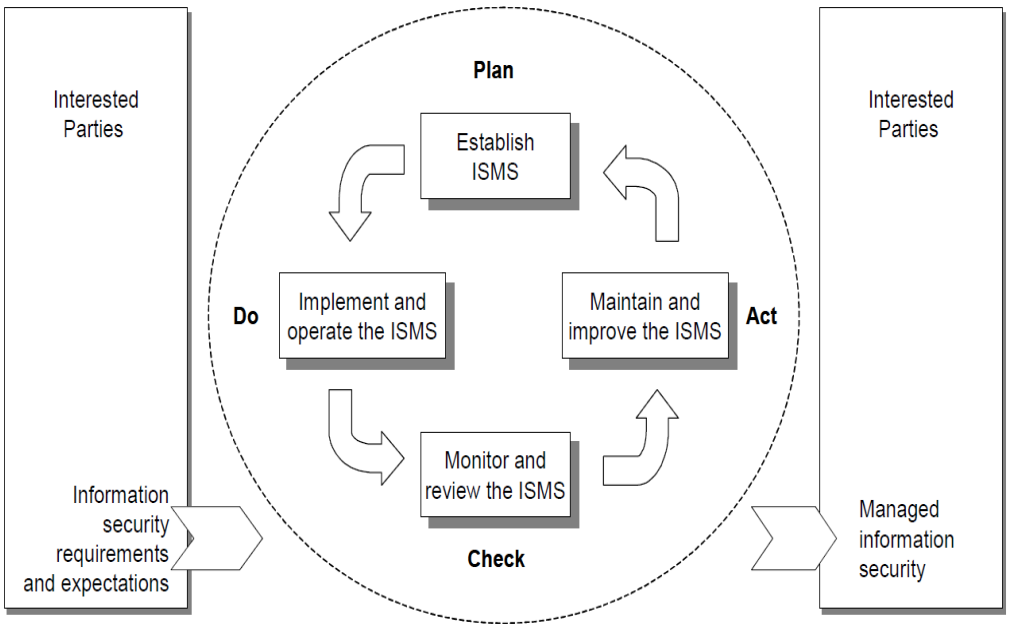
Η μέθοδος που θα ακολουθηθεί στην μελέτη της ασφάλειας του "HOSPITAL" είναι η OCTAVE. Η μέθοδος OCTAVE είναι δημιουργία της ομάδας CERT Survivable Enterprise Management η οποία ανήκει στο Software Engineering Institute (SEI) του Carnegie Mellon University με σκοπό να αποτελέσει ένα εργαλείο αξιολόγησης της ασφάλειας των πληροφοριακών συστημάτων ενός οργανισμού. Ειδικότερα θα χρησιμοποιηθεί η έκδοση Octave Allegro.

Κεφάλαιο 4
ISO/IEC 27001:2005

Το πρότυπο του Διεθνή Οργανισμού Τυποποίησης (International Organization for Standardization - ISO), **ISO/IEC 27001:2005 «Information technology – Security techniques – Information security management systems – Requirements»** ορίζει ένα μοντέλο για τη δημιουργία, υλοποίηση, λειτουργία, παρακολούθηση, διατήρηση και βελτίωση ενός Συστήματος Διαχείρισης της Ασφάλειας της Πληροφορίας (Information Security Management System – ISMS), σε ένα οργανισμό. Οι απαιτήσεις που καθορίζονται από το ISO/IEC 27001 είναι κατάλληλες για κάθε είδος οργανισμού ανεξάρτητα από τη φύση και το μέγεθός του.

4.1 Περιγραφή της μεθοδολογίας

Για την ανάπτυξη ενός ISMS, το πρότυπο υιοθετεί το μοντέλο Plan-Do-Check-Act (PDCA).



Σχήμα 4.1: Εφαρμογή του PDCA μοντέλου για την ανάπτυξη ISMS

Σύμφωνα με το μοντέλο PDCA:

Καθορίζεται (Plan) το ISMS. Ορίζονται οι πολιτικές, στόχοι, διεργασίες και διαδικασίες σχετικές με την διαχείριση κινδύνων και την ασφάλεια των πληροφοριών στον οργανισμό.

Εφαρμόζεται (Do) το ISMS. Δημιουργείται και εκτελείται το ISMS.

Ελέγχεται (Check) το ISMS. Αξιολογείται η απόδοση του ISMS και γίνεται αναθεώρηση όπου είναι απαραίτητο.

Ενεργούνται (Act) βελτιωτικές πράξεις στο ISMS. Με βάση τον έλεγχο διενεργούνται διορθωτικές και βελτιωτικές ενέργειες.

Οι έλεγχοι (controls) που πρέπει να υλοποιήσει ένας οργανισμός σύμφωνα με το πρότυπο είναι οι παρακάτω. Η ταξινόμηση των ελέγχων είναι αυτή που ακολουθεί και το πρότυπο.

4. ISMS

4.1 Γενικές Απαιτήσεις

Ο οργανισμός πρέπει να εγκαθιστά, να εφαρμόζει, λειτουργεί, παρακολουθεί, αξιολογεί, διατηρεί και βελτιώνει τεκμηριωμένο ISMS στο πλαίσιο της συνολικής επιχειρηματικής δραστηριότητας του οργανισμού και των κινδύνων που αντιμετωπίζει. Για τους σκοπούς του παρόντος διεθνούς προτύπου η μέθοδος που χρησιμοποιείται βασίζεται στο μοντέλο PDCA.

4.2 Establishing and Managing

4.2.1 Plan: Για τον καθορισμό του ISMS θα πρέπει:

Να καθοριστούν ο σκοπός, η έκταση και τα όρια του ISMS στον οργανισμό.

Να καθοριστεί η πολιτική του ISMS έτσι ώστε:

Να ορίζει το πλαίσιο, τους στόχους, τις οδηγίες και τις αρχές που αφορούν στην ασφάλεια της πληροφορίας

Να λαμβάνει υπόψη τις απαιτήσεις εργασίας, νομικές και κανονιστικές απαιτήσεις και τις συμβατικές υποχρεώσεις για ασφάλεια.

Να συμμορφώνεται με το σχέδιο διαχείρισης κινδύνου του οργανισμού.

Να καθορίζει κριτήρια αξιολόγησης του κινδύνου (βλ. 4.2.1 c).

Να παίρνει την έγκριση της διοίκησης.

Να καθοριστεί η προσέγγιση εκτίμησης κινδύνου ως εξής:

Προσδιορίζεται η κατάλληλη μεθοδολογία αξιολόγησης κινδύνων.

Καθορίζονται τα κατάλληλα κριτήρια για την αποδοχή κινδύνων και αποδεκτών επιπέδων κινδύνων (βλ. 5.1 f).

Να προσδιοριστούν οι κίνδυνοι με τα εξής βήματα:

- Προσδιορισμός των αγαθών του οργανισμού και των ιδιοκτητών τους.
- Προσδιορισμός των απειλών για τα αγαθά αυτά.
- Προσδιορισμός των ευπαθειών των αγαθών.
- Προσδιορισμός της επίπτωσης που επιφέρει η απώλεια της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των αγαθών.

Να γίνει ανάλυση και εκτίμηση των κινδύνων με τις παρακάτω ενέργειες:

- Γίνεται αξιολόγηση των επιπτώσεων στον οργανισμό της παραβίασης ασφάλειας των ιδιοτήτων των αγαθών.
- Γίνεται εκτίμηση της πιθανότητας να συμβεί παραβίαση ασφάλειας συνδυάζοντας την απειλή για ένα αγαθό, την ευπάθειά του και την επίπτωση που θα έχει στον οργανισμό.
- Υπολογίζεται το επίπεδο των κινδύνων.
- Προσδιορίζονται ποιοι κίνδυνοι θα αντιμετωπιστούν και ποιοι είναι αποδεκτοί (βλ. 4.2.1 c 2).

Να προσδιοριστούν και να αξιολογηθούν οι επιλογές αντιμετώπισης των κινδύνων. Τέτοιες επιλογές μπορεί να είναι:

- Εφαρμογή κατάλληλων ελέγχων
- Συνειδητή και αντικειμενική αποδοχή των κινδύνων.
- Αποφυγή των κινδύνων.
- Μεταφορά των κινδύνων σε τρίτους (ασφάλεια κλπ.)

Να επιλεχθούν τα αντικείμενα ελέγχου και οι έλεγχοι για την αντιμετώπιση του κινδύνου. (Παράρτημα Α΄)

Να λαμβάνουν την έγκριση της διοίκησης για τους αποδεκτούς υπολειπόμενους κινδύνους.

Να έχουν λάβει την έγκριση της διοίκησης για την εφαρμογή και λειτουργία του ISMS.

Να ετοιμαστεί μια Δήλωση Εφαρμογής η οποία θα περιλαμβάνει:

Τα αντικείμενα ελέγχου, οι επιλεγμένοι έλεγχοι στο 4.2.1 g και οι λόγοι επιλογής τους.

Τα αντικείμενα ελέγχου και οι έλεγχοι που εφαρμόζονται στο παρόν (βλ. 4.2.1 e 2).

Τις εξαιρέσεις αντικειμένων ελέγχου και ελέγχων από αυτά που αναφέρονται στο Παράρτημα Α΄.

4.2.2. Do: Για την εφαρμογή και λειτουργία του ISMS οργανισμός πρέπει να κάνει τα εξής:

Να διατυπώσει ένα σχέδιο αντιμετώπισης κινδύνου (βλ. 5).

Να εφαρμόσει το σχέδιο αντιμετώπισης κινδύνου.

Να εφαρμόσει τους ελέγχους που επιλέχθηκαν στο 4.2.1 g και ανταποκρίνονται στα αντικείμενα των ελέγχων.

Να καθορίσει κριτήρια μέτρησης αποτελεσματικότητας και διαδικασίες αξιολόγησης της αποτελεσματικότητας (βλ. 4.2.3 c).

Να εφαρμόσει προγράμματα κατάρτισης και ευαισθητοποίησης σε θέματα ασφάλειας στο προσωπικό (βλ 5.2.2).

Διαχείριση της λειτουργίας του ISMS.

Διαχείριση των πόρων για το ISMS.

Να εφαρμόσει διαδικασίες και ελέγχους ανίχνευσης περιστατικών παραβίασης της ασφάλειας και αντιμετώπισής τους.

4.2.3 Check: Για την παρακολούθηση και επανεξέταση του ISMS ο οργανισμός πρέπει να κάνει τα εξής:

Παρακολούθηση, επανεξέταση και έλεγχο των διαδικασιών για να:

- Ανιχνεύονται άμεσα σφάλματα στα αποτελέσματα της διαδικασίας.

- Εντοπίζονται άμεσα ρήγματα και περιστατικά ασφάλειας επιτυχημένα ή όχι.
- Αξιολογεί η διοίκηση την απόδοση των μέτρων ασφάλειας.
- Ανιχνεύει περιστατικά ασφάλειας κάνοντας χρήση των ενδείξεων ώστε να τα προλαμβάνει.
- Προσδιορίζει αν ήταν αποτελεσματικές οι ενέργειες που έγιναν για την αντιμετώπιση ενός ρήγματος ασφάλειας.

Προβαίνει σε τακτικές αξιολογήσεις της αποτελεσματικότητας του ISMS.

Μετρά την αποτελεσματικότητα των ελέγχων για να εξακριβώσει ότι τηρήθηκαν οι απαιτήσεις ασφάλειας.

Αξιολογεί σε τακτά χρονικά διαστήματα την ανάλυση κινδύνου και τους ανεκτούς υπολειπόμενους κινδύνους λαμβάνοντας υπόψη αλλαγές:

- Στον οργανισμό.
- Στην τεχνολογία.
- Στους επιχειρηματικούς στόχους και διαδικασίες.
- Στις εντοπισμένες απειλές.
- Στην αποτελεσματικότητα των εφαρμοσμένων ελέγχων.
- Σε εξωτερικά γεγονότα όπως αλλαγή νομοθεσίας, αλλαγή συμβατικών υποχρεώσεων και κοινωνικές αλλαγές.

Διενεργεί σε τακτά χρονικά διαστήματα εσωτερικούς ελέγχους του ISMS (βλ. 6).

Προβαίνει σε τακτά χρονικά διαστήματα σε αξιολόγηση του ISMS για να εξασφαλιστεί ότι η έκταση εφαρμογής του είναι επαρκής και προσδιορίζονται βελτιώσεις στο ISMS (βλ. 7.1).

Αναβαθμίζει τα σχέδια ασφάλειας σύμφωνα με τα ευρήματα της παρακολούθησης και της αξιολόγησης.

Καταγράφει πράξεις και συμβάντα που μπορεί να επηρεάσουν την αποτελεσματικότητα του ISMS.

4.2.4 Act: Για τη Συντήρηση και βελτίωση του ISMS ο οργανισμός θα πρέπει τακτικά να κάνει τα εξής:

- Εφαρμόζει τις καθορισμένες βελτιώσεις του ISMS.
- Λαμβάνει τα κατάλληλα διορθωτικά και προληπτικά μέτρα (σύμφωνα με τα 8.2 και 8.3).
- Κοινοποιεί τα μέτρα και τις βελτιώσεις σε όλους τους ενδιαφερόμενους.
- Εξασφαλίζει ότι οι βελτιώσεις πληρούν τους επιδιωκόμενους στόχους.

4.3 Απαιτήσεις Τεκμηρίωσης

4.3.1 Γενικά

- Η τεκμηρίωση του ISMS περιλαμβάνει:
- Τεκμηριωμένες δηλώσεις της πολιτικής του ISMS και των στόχων (βλ. 4.2.1b).
- Το πεδίο εφαρμογής του ISMS (βλ. 4.2.1a).
- Διαδικασίες και ελέγχους για την υποστήριξη του ISMS.
- Περιγραφή της μεθοδολογίας ανάλυσης κινδύνου (βλ. 4.2.1c).
- Την έκθεση ανάλυσης κινδύνου (βλ. 4.2.1c έως 4.2.1g).
- Το σχέδιο αντιμετώπισης του κινδύνου (βλ. 4.2.2 b)

Τεκμηριωμένες διαδικασίες για να διασφαλίσει ο οργανισμός τον αποτελεσματικό σχεδιασμό, λειτουργία και έλεγχο των διαδικασιών του ISMS και τον τρόπο μέτρησης της αποτελεσματικότητας.

Αρχεία που απαιτούνται από το πρότυπο (βλ. 4.3.3)

Η Δήλωση Εφαρμογής.

4.3.2 Έλεγχος των εγγράφων. Τα απαιτούμενα έγγραφα για το ISMS πρέπει να προστατεύονται και να ελέγχονται. Πρέπει να καθοριστεί μια τεκμηριωμένη διαδικασία που ορίζει τις ενέργειες της διοίκησης για να:

- Εγκρίνει τα έγγραφα για την επάρκειά τους πριν την έκδοση
- Επανεξετάσει, ενημερώσει και επαν-εγκρίνει τα έγγραφα.
- Αναγνωρίζει τις αλλαγές και αναθεωρήσεις των εγγράφων.
- Εξασφαλίζει ότι τα αναθεωρημένα έγγραφα είναι διαθέσιμα όπου απαιτείται.
- Εξασφαλίζει ότι τα έγγραφα είναι ευανάγνωστα και άμεσα αναγνωρίσιμα.
- Εξασφαλίζει τη διαθεσιμότητα των εγγράφων και τη διαχείρισή τους ανάλογα με τη διαβάθμισή τους.
- Εξασφαλίζει ότι αναγνωρίζονται τα έγγραφα εξωτερικής προέλευσης.
- Εξασφαλίζει ότι η διανομή των εγγράφων είναι ελεγχόμενη.
- Αποτρέπει τη χρήση των παρωχημένων εγγράφων.
- Εφαρμόζει κατάλληλη αναγνώριση στα παραπάνω αν διατηρούνται για οποιοδήποτε σκοπό.

4.3.3 Έλεγχος των αρχείων. Τα αρχεία πρέπει να τηρούνται και να διατηρούνται για να παρέχουν αποδεικτικά στοιχεία της συμμόρφωσης με τις απαιτήσεις του ISMS. Θα πρέπει να προστατεύονται και να ελέγχονται. Το ISMS πρέπει να λαμβάνει υπόψη τυχόν σχετικές νομικές ή κανονιστικές απαιτήσεις και τις συμβατικές υποχρεώσεις. Τα αρχεία πρέπει να παραμένουν ευανάγνωστα, ευκόλως αναγνωρίσιμα και ανακτήσιμα. Οι έλεγχοι που απαιτούνται για την αναγνώριση, αποθήκευση, προστασία, ανάκτηση, τη διατήρηση στο χρόνο και τη διάθεση των αρχείων θα πρέπει να τεκμηριώνονται και να εφαρμόζονται. Παραδείγματα εγγραφών είναι ένα βιβλίο επισκεπτών, εκθέσεις ελέγχου και συμπληρωμένα έντυπα άδειας πρόσβασης.

5. ΕΥΘΥΝΗ ΔΙΟΙΚΗΣΗΣ

5.1 Δέσμευση της διοίκησης

Η Διοίκηση θα πρέπει να παράσχει αποδεικτικά στοιχεία δέσμευσής της για τη δημιουργία, υλοποίηση, τη λειτουργία, την παρακολούθηση, την αξιολόγηση, τη συντήρηση και τη βελτίωση της ISMS με:

- Τη δημιουργία μιας ISMS πολιτικής.
- Τη βεβαίωση ότι είναι καθορισμένοι οι στόχοι και τα σχέδια του ISMS.
- Τον καθορισμό των ρόλων και των ευθυνών για την ασφάλεια των πληροφοριών.
- Την ευαισθητοποίηση του προσωπικού για τη σημασία της επίτευξης των στόχων της ασφάλειας των πληροφοριών στον οργανισμό και τη συμμόρφωση σύμφωνα με την πολιτική της ασφάλειας των πληροφοριών, τις ευθύνες του σύμφωνα με το δίκαιο και την ανάγκη για συνεχή βελτίωση στον τομέα αυτό.
- Την παροχή επαρκών πόρων για την καθιέρωση, εφαρμογή, λειτουργία, παρακολούθηση, αξιολόγηση, διατήρηση και βελτίωση της ISMS (βλ. 5.2.1).
- Τον καθορισμό κριτηρίων για την αποδοχή των κινδύνων και τα αποδεκτά επίπεδα κινδύνου.
- Την εξασφάλιση ότι πραγματοποιούνται οι εσωτερικοί έλεγχοι ISMS (βλ. 6)
- Τη διεξαγωγή επανεξέτασης του ISMS (βλ. 7).

5.2 Διαχείριση των πόρων

5.2.1 Παροχή πόρων

Ο οργανισμός πρέπει να καθορίζει και να παρέχει τους πόρους που απαιτούνται για:

- Θέσπιση, εφαρμογή, λειτουργία, παρακολούθηση, έλεγχος, διατήρηση και βελτίωση του ISMS.
- Να εξασφαλίζει ότι οι διαδικασίες ασφάλειας των πληροφοριών υποστηρίζουν τις επιχειρηματικές απαιτήσεις.
- Τον εντοπισμό και την συμμόρφωση των νομικών και κανονιστικών απαιτήσεων και των συμβατικών υποχρεώσεων της ασφάλειας
- Την επίτευξη ασφάλειας με τη σωστή εφαρμογή όλων των εφαρμοσμένων ελέγχων
- Τη διενέργεια περιοδικών επιθεωρήσεων, όταν χρειάζεται, και κατάλληλη αντιμετώπιση στα αποτελέσματα αυτών των κριτικών
- Να βελτιώσει την αποτελεσματικότητα της ISMS, όπου απαιτείται.

5.2.2 Εκπαίδευση, ευαισθητοποίηση και επάρκεια

Ο οργανισμός οφείλει να εξασφαλίζει ότι όλο το προσωπικό στο οποίο έχουν ανατεθεί καθήκοντα που ορίζονται από το ISMS είναι ικανά για την εκτέλεσή τους με:

- Τον καθορισμό των αναγκαίων δεξιοτήτων για το προσωπικό που εκτελεί εργασίες που επηρεάζουν την ISMS.
- Την παροχή κατάρτισης και άλλες δράσεις για να ικανοποιηθούν οι παραπάνω ανάγκες
- Την αξιολόγηση της αποτελεσματικότητας των δράσεων που αναλαμβάνονται
- Την διατήρηση αρχείων της εκπαίδευσης, της κατάρτισης, των δεξιοτήτων, την εμπειρία και των προσόντων (βλ. 4.3.3).

Ο οργανισμός πρέπει επίσης να διασφαλίζει ότι όλο το σχετικό προσωπικό γνωρίζει τις αρμοδιότητες και τη σημασία των δραστηριοτήτων ασφάλειας των πληροφοριών και πώς αυτοί συμβάλλουν στην επίτευξη των στόχων ISMS.

6. ΕΣΩΤΕΡΙΚΟΙ ΕΛΕΓΧΟΙ ISMS

Ο οργανισμός πρέπει να διενεργεί εσωτερικούς ελέγχους ISMS σε τακτά χρονικά διαστήματα για να διαπιστωθεί αν οι στόχοι, οι έλεγχοι, οι διεργασίες και οι διαδικασίες του ISMS:

- Συμμορφώνονται με τις απαιτήσεις του παρόντος διεθνούς προτύπου και τις σχετικές νομοθετικές και κανονιστικές διατάξεις
- Συμμορφώνονται με τις καθορισμένες απαιτήσεις ασφάλειας των πληροφοριών
- Έχουν αποτελεσματική εφαρμογή και διατήρηση
- Λειτουργούν όπως αναμένεται.

Ένα πρόγραμμα ελέγχου πρέπει να σχεδιάζεται, λαμβάνοντας υπόψη την κατάσταση και τη σημασία των διαδικασιών και των περιοχών που πρόκειται να ελεγχθούν, καθώς και τα αποτελέσματα προηγούμενων ελέγχων. Τα κριτήρια ελέγχου, το πεδίο εφαρμογής, η συχνότητα και οι μέθοδοι θα πρέπει να οριστούν. Η επιλογή των ελεγκτών και η διενέργεια των ελέγχων

πρέπει να εξασφαλίζουν την αντικειμενικότητα και την αμεροληψία της διαδικασίας ελέγχου. Οι ελεγκτές δεν θα ελέγχουν τη δική τους εργασία.

Οι ευθύνες και οι απαιτήσεις για το σχεδιασμό και τη διεξαγωγή ελέγχων, καθώς και για την αναφορά των αποτελεσμάτων και τη διατήρηση αρχείων (βλ. 4.3.3) θα πρέπει να ορίζεται σε μια τεκμηριωμένη διαδικασία.

Η διοίκηση που είναι υπεύθυνη για το πεδίο που ελέγχεται, πρέπει να εξασφαλίσει ότι δράσεις λαμβάνονται χωρίς αδικαιολόγητη καθυστέρηση για να εξαλείψουν τις περιπτώσεις μη συμμόρφωσης που εντοπίζονται και τα αίτιά τους. Η παρακολούθηση των δραστηριοτήτων πρέπει να περιλαμβάνει την επαλήθευση των ενεργειών και την υποβολή εκθέσεων σχετικά με τα αποτελέσματα ελέγχου (βλ. 8).

7. ΔΙΟΙΚΗΤΙΚΗ ΑΞΙΟΛΟΓΗΣΗ ΤΟΥ ISMS

7.1 Γενικά

Η Διοίκηση θα πρέπει να επανεξετάζει την ISMS του οργανισμού σε τακτά χρονικά διαστήματα (τουλάχιστον μια φορά το χρόνο) για να εξασφαλιστεί η συνεχής καταλληλότητα, επάρκεια και αποτελεσματικότητα. Αυτή η αξιολόγηση πρέπει να περιλαμβάνει εκτίμηση των δυνατοτήτων βελτίωσης και την ανάγκη για αλλαγές στην ISMS, συμπεριλαμβανομένης της πολιτικής για την ασφάλεια των πληροφοριών και των στόχων της ασφάλειας των πληροφοριών. Τα αποτελέσματα των αξιολογήσεων θα πρέπει να τεκμηριώνονται σαφώς και πρέπει να διατηρούνται σε αρχεία (βλ. 4.3.3).

7.2 Δεδομένα Αξιολόγησης

Τα δεδομένα για την διοικητική αξιολόγηση πρέπει να περιλαμβάνουν:

- Τα αποτελέσματα των ελέγχων του ISMS και σχόλια.
- Πληροφορίες από τα ενδιαφερόμενα μέρη.
- Τεχνικές, προϊόντα ή διαδικασίες, οι οποίες θα μπορούσαν να χρησιμοποιηθούν από τον οργανισμό για τη βελτίωση της απόδοσης και αποτελεσματικότητας του ISMS.
- Το καθεστώς των προληπτικών και διορθωτικών ενεργειών.

- Τα τρωτά σημεία και τις απειλές που δεν αντιμετωπίζονται επαρκώς από την προηγούμενη ανάλυση επικινδυνότητας.
- Τα αποτελέσματα από μετρήσεις αποτελεσματικότητας.
- Επακόλουθες ενέργειες προηγούμενων αξιολογήσεων.
- Αλλαγές που θα μπορούσαν να επηρεάσουν την ISMS
- Προτάσεις για βελτίωση.

7.3 Αποτελέσματα Αξιολόγησης

Τα αποτελέσματα από την διοικητική αξιολόγηση θα πρέπει να περιλαμβάνουν αποφάσεις και ενέργειες σχετικές με τα παρακάτω.

Βελτίωση της αποτελεσματικότητας του ISMS

Ενημέρωση της ανάλυσης επικινδυνότητας και του σχεδίου Ασφάλειας.

Τροποποίηση των διαδικασιών και των ελέγχων που επηρεάζουν την ασφάλεια των πληροφοριών, εφόσον είναι αναγκαίο για να ανταποκρίνεται στα εσωτερικά ή εξωτερικά γεγονότα που ενδέχεται να επηρεάσουν την ISMS, συμπεριλαμβανομένων των αλλαγών σε:

- Τις απαιτήσεις της επιχείρησης.
- Τις απαιτήσεις ασφάλειας.
- Επιχειρηματικές διαδικασίες που επηρεάζουν τις υπάρχουσες απαιτήσεις.
- Ρυθμιστικές ή νομικές απαιτήσεις.
- Τις συμβατικές υποχρεώσεις.
- Τα επίπεδα του κινδύνου ή/και τα κριτήρια για την αποδοχή των κινδύνων.
- Τους πόρους που θα χρειαστούν.
- Βελτίωση στο τρόπο μέτρησης της αποτελεσματικότητα των ελέγχων.

8. ΒΕΛΤΙΩΣΗ ΤΟΥ ISMS

8.1 Συνεχής βελτίωση

Ο οργανισμός πρέπει να βελτιώνει συνεχώς την αποτελεσματικότητα του ISMS, μέσω της χρήσης των πληροφοριών πολιτικής ασφάλειας, τους στόχους της ασφάλειας των πληροφοριών, τα αποτελέσματα του ελέγχου, της ανάλυσης των περιστατικών που έχουν καταγραφεί, τις διορθωτικές και προληπτικές δράσεις και τη διοικητική αξιολόγηση (βλέπε σημείο 7).

8.2 Διορθωτικές ενέργειες

Ο οργανισμός πρέπει να αναλάβει δράση για την εξάλειψη της αιτίας της μη συμμόρφωσης με τις απαιτήσεις στην ISMS προκειμένου να αποτραπεί η επανάληψη της. Η τεκμηριωμένη διαδικασία για διορθωτικές ενέργειες πρέπει να καθορίζει τις απαιτήσεις για:

Ο οργανισμός πρέπει να αναλάβει δράση για την εξάλειψη της αιτίας της μη συμμόρφωσης με τις απαιτήσεις στην ISMS προκειμένου να αποτραπεί η επανάληψη της. Η τεκμηριωμένη διαδικασία για διορθωτικές ενέργειες πρέπει να καθορίζει τις απαιτήσεις για:

- Τον εντοπισμό ασυμφωνιών.
- Τον προσδιορισμό των αιτίων των μη συμμορφώσεων
- Αξιολόγηση της ανάγκης για δράσεις για να εξασφαλιστεί ότι οι μη συμμορφώσεις δεν θα επαναληφθούν
- Τον καθορισμό και την εφαρμογή των διορθωτικών μέτρων που απαιτούνται
- Την καταγραφή των αποτελεσμάτων των δράσεων που αναλαμβάνονται (βλ. 4.3.3)
- Την αναθεώρηση των διορθωτικών μέτρων που λαμβάνονται

8.3 Προληπτική δράση

Ο οργανισμός πρέπει να προβαίνει σε ενέργειες για την εξάλειψη της αιτίας των πιθανών περιπτώσεων μη συμμόρφωσης με τις απαιτήσεις του ISMS, προκειμένου να αποφευχθεί η επανεμφάνισή τους. Οι προληπτικές δράσεις θα πρέπει να είναι κατάλληλες για τις επιπτώσεις

από τα πιθανά προβλήματα. Η τεκμηριωμένη διαδικασία για την προληπτική δράση πρέπει να καθορίζει τις απαιτήσεις για:

- Τον εντοπισμό πιθανών περιπτώσεων μη συμμόρφωσης, καθώς και τις αιτίες τους.
- Αξιολογεί την ανάγκη ανάληψης δράσης για την πρόληψη της εμφάνισης των μη συμμορφώσεων.
- Τον καθορισμό και την εφαρμογή των προληπτικών μέτρων που απαιτούνται.
- Τα αποτελέσματα της καταγραφής των ενεργειών που έχουν λάβει δράση (βλ. 4.3.3).
- Την επανεξέταση των ληφθέντων προληπτικών μέτρων
- Ο οργανισμός πρέπει να εντοπίζει τους αλλαγμένους κινδύνους και να εντοπίσει τις προληπτικές δράσεις που απαιτούνται εστιάζοντας την προσοχή του στους σημαντικά αλλαγμένους κινδύνους.
- Η προτεραιότητα των προληπτικών ενεργειών θα πρέπει να καθορίζεται με βάση τα αποτελέσματα της ανάλυσης επικινδυνότητας.

Στόχοι ελέγχου και χειριστήρια

Στο παράρτημα Α του προτύπου περιγράφονται αναλυτικά οι στόχοι και τα μέτρα που πρέπει να ληφθούν για την επίτευξή τους. Οι στόχοι και τα μέτρα ευθυγραμμίζονται με αυτά που περιγράφονται στο ISO / IEC 27002:2005 και πρέπει να επιλέγονται ως μέρος της διαδικασίας που ορίζεται στο 4.2.1

Κεφάλαιο 5
OCTAVE Allegro

Η μέθοδος OCTAVE (**O**perationally **C**ritical **T**hreat, **A**sset, and **V**ulnerability **E**valuation) είναι μια **ποιοτική** μέθοδος εκτίμησης κινδύνου που αναπτύχθηκε στο SEI σε συνεργασία με το Telemedicine and Advanced Technology Research Center (TATRC) το 1999. Σκοπός της μεθόδου ήταν να αποτελέσει ένα εργαλείο για το U.S. Department of Defense (DoD) εφαρμογής του νόμου Health Insurance Portability and Accountability Act (HIPAA, Αύγουστος 1996) για τη μυστικότητα και ασφάλεια των πληροφοριών στο χώρο της υγείας. [23]

5.1 Εξέλιξη της OCTAVE

Από το 1999 που εμφανίστηκε πρώτη φορά, υπήρξαν αλλαγές και διαφορετικές εκδόσεις της μεθόδου οι οποίες παρουσιάζονται στον πίνακα 5.1.

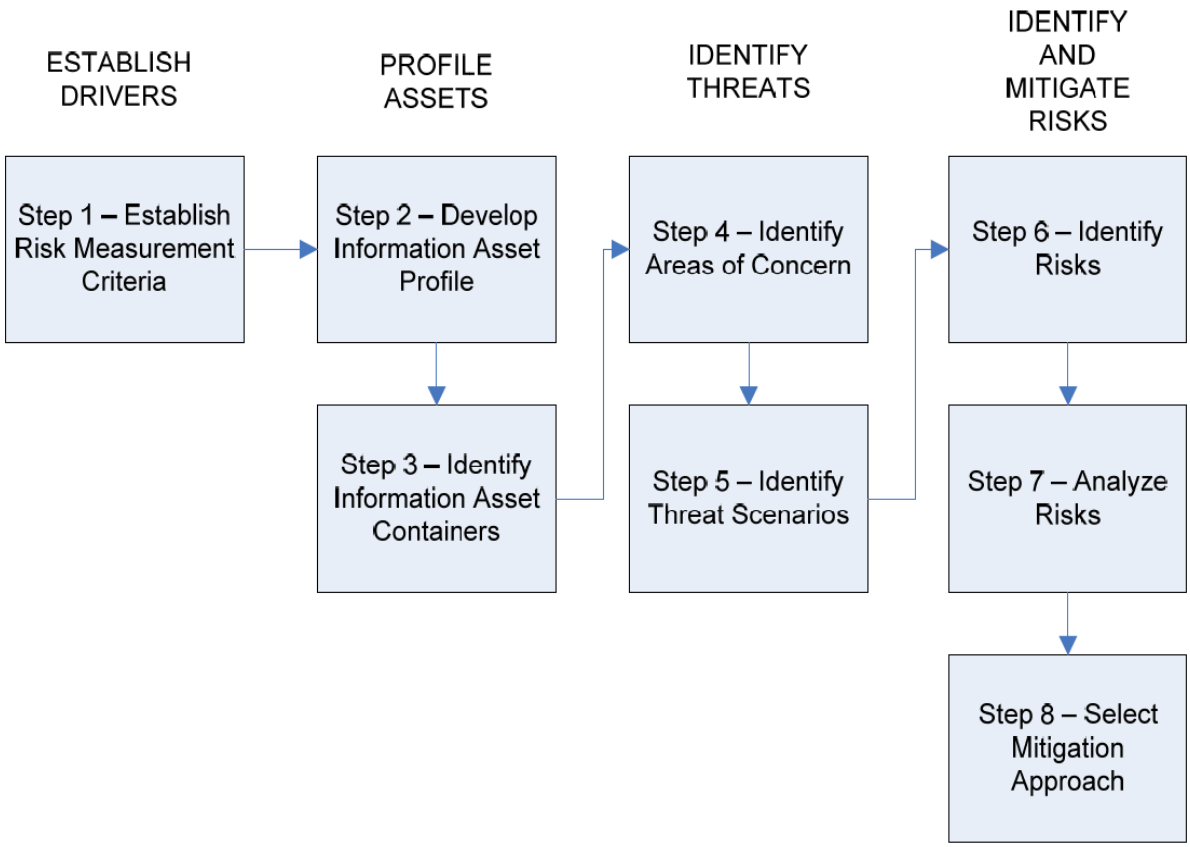
Date	Publication Title
September 1999	OCTAVE Framework, Version 1.0
September 2001	OCTAVE Framework, Version 2.0
December 2001	OCTAVE Criteria, Version 2.0
September 2003	OCTAVE-S v0.9
March 2005	OCTAVE-S v1.0
June 2007	Introduction of OCTAVE Allegro v1.0

Πίνακας 5.1: Εκδόσεις της μεθόδου OCTAVE

Η τελευταία εξέλιξη της μεθόδου OCTAVE είναι η OCTAVE Allegro. Η μέθοδος OCTAVE Allegro απλουστεύει και βελτιστοποιεί την διαδικασία αξιολόγησης της ασφάλειας των πληροφοριακών συστημάτων. Δίνει προτεραιότητα στις πληροφορίες των συστημάτων και μελετάει τους πόρους του οργανισμού (τεχνολογία, ανθρώπους, εγκαταστάσεις) σε σχέση με το πληροφοριακό σύστημα και τις διαδικασίες και σκοπούς που υποστηρίζουν. Ελαχιστοποιεί τους απαιτούμενους πόρους σε ανθρώπινο δυναμικό και εργατοώρες για να υλοποιήσει την εκτίμηση κινδύνων. [22]

5.2 Περιγραφή της OCTAVE Allegro

Η μέθοδος αποτελείται από 4 φάσεις οι οποίες υλοποιούνται σε 8 βήματα (Πίνακας 5.1). Τα εξαγόμενα κάθε φάσεις αποτελούν δεδομένα για την επόμενη φάση.



Εικόνα 5.1.: Φάσεις και βήματα μεθόδου OCTAVE ALLEGRO

Φάση 1. Καθορισμός οδηγών (Establish Drivers)

1ο Βήμα (Step 1). Καθορισμός κριτηρίων μέτρησης του κινδύνου (Establish Risk Measurement Criteria): Στο βήμα αυτό διενεργούνται 2 δραστηριότητες.

1η Δραστηριότητα (Activity 1): Καθορίζεται ένα σύνολο ποιοτικών κριτηρίων και των παραμέτρων που τα καθορίζουν σύμφωνα με τα οποία θα αξιολογηθούν οι επιπτώσεις των κινδύνων στον οργανισμό. Το ελάχιστο σύνολο κριτηρίων μετρήσεων μπορεί να είναι το παρακάτω:

1. Φήμη/Εμπιστοσύνη πελατών (Reputation/Customer confidence)
2. Οικονομικά (Financial)
3. Παραγωγικότητα (Productivity)
4. Ασφάλεια και υγεία(Safety and health)
5. Πρόστιμα και νομικές ποινές (Fines/Legal penalties)
6. Καθορισμένες από το χρήστη (User-defined impact area)

2η Δραστηριότητα (Activity 2): Ταξινόμηση των περιοχών κατά φθίνουσα σειρά.

Φάση 2. Προφίλ των Αγαθών (Profile Assets)

2ο Βήμα (Step 2). Δημιουργία των Προφίλ των Πληροφοριακών Αγαθών (Develop Information Asset Profile): Στο βήμα αυτό διενεργούνται 8 δραστηριότητες.

1η Δραστηριότητα (Activity 1): Προσδιορίζεται ένα σύνολο πληροφοριακών αγαθών στα οποία μπορεί να γίνει αξιολόγηση. Αυτό μπορεί να γίνει απαντώντας στα εξής ερωτήματα:

- Ποια πληροφοριακά αγαθά είναι τα σημαντικότερα στον οργανισμό;
- Ποια πληροφοριακά αγαθά χρησιμοποιούνται καθημερινά;
- Ποια πληροφοριακά αγαθά αν χαθούν διακόπτουν τη λειτουργία του οργανισμού;
- Ποια άλλα πληροφοριακά αγαθά σχετίζονται με τα παραπάνω;

2η Δραστηριότητα (Activity 2): Εστίαση στα λίγα κρίσιμα (Focusing on the critical few). Για να γίνει η επιλογή των κρίσιμων αγαθών από αυτά που προέκυψαν από την Δραστηριότητα 1, θα πρέπει να καθοριστεί ποιο από αυτά θα προκαλέσει δυσμενείς επιπτώσεις στον οργανισμό, αν του συμβεί κάτι από τα παρακάτω:

1. Αποκάλυψη (disclose) σε μη εξουσιοδοτημένα άτομα
2. Τροποποίηση (modified) από μη εξουσιοδοτημένα άτομα
3. Απώλεια ή καταστροφή (Loss/Destroy)
4. Διακοπή (Interrupt) πρόσβασης

Στις επόμενες 3 έως 8 δραστηριότητες γίνεται συλλογή πληροφοριών για τα προς αξιολόγηση αγαθά με τη χρήση του Φύλλου Εργασίας - Φ.Ε. (Worksheet) 8: Critical Information Asset Profile.

3η Δραστηριότητα (Activity 3): Στη στήλη 1 εγγράφουμε το όνομα του αγαθού.

4η Δραστηριότητα (Activity 4): Στη στήλη 2 εγγράφουμε το λόγο επιλογής του αγαθού. Για την αιτιολογία απαντάμε στα παρακάτω ερωτήματα:

Γιατί το αγαθό είναι κρίσιμο για τον οργανισμό;

Υπόκειται το αγαθό στις κανονιστικές απαιτήσεις;

5η Δραστηριότητα (Activity 5): Στη στήλη 3 εγγράφουμε την περιγραφή του αγαθού. Για την περιγραφή απαντάμε στα παρακάτω ερωτήματα:

- Ποια είναι η συνηθισμένη ονομασία του αγαθού (στους ανθρώπους του οργανισμού);
- Είναι σε ηλεκτρονική μορφή, φυσική (π.χ. χαρτί) ή και τα δύο;
- Υπάρχουν παράγοντες που χαρακτηρίζουν εξειδικευμένα το αγαθό (π.χ. νόμοι);
- Ποιες διαδικασίες ή υπηρεσίες υποστηρίζονται από αυτό το αγαθό;

6η Δραστηριότητα (Activity 6): Στη στήλη 4 εγγράφουμε τους ιδιοκτήτες του κρίσιμου αγαθού. Για την περιγραφή απαντάμε στα παρακάτω ερωτήματα:

- Ποιος στον οργανισμό έχει την κύρια ευθύνη για το αγαθό;
- Σε ποιον ανήκει η διαδικασία στην οποία το αγαθό χρησιμοποιείται;
- Ποιος ορίζει την αξία (χρηματική ή άλλη) του αγαθού;
- Σε ποιον θα υπήρχε η μεγαλύτερη επίπτωση αν στο αγαθό συμβεί παραβίαση ασφάλειας;
- Υπάρχουν διαφορετικοί ιδιοκτήτες για τα συστατικά στοιχεία-δεδομένα που συνθέτουν το αγαθό;
- Ανήκει το αγαθό σε περισσότερα του ενός τμήματα του οργανισμού;
- Ποια είναι η θέση του ιδιοκτήτη στον οργανισμό;

7η Δραστηριότητα (Activity 7): Στη στήλη 5 εγγράφουμε τις απαιτήσεις ασφάλειας για τις ιδιότητες του αγαθού:

Εμπιστευτικότητα (Confidentiality)

Ακεραιότητα (Integrity)

Διαθεσιμότητα (Availability)

Οι απαιτήσεις ασφάλειας θα πρέπει να συμμορφώνονται με τυχόν κανονισμούς και νομοθεσία που αφορούν στο αγαθό.

8η Δραστηριότητα (Activity 8): Στη στήλη 6 επιλέγουμε την σημαντικότερη απαίτηση ασφάλειας (τσεκάροντας με ένα Χ το κατάλληλο).

3ο Βήμα (Step 3). Καθορισμός των Περιεκτών των Πληροφοριακών Αγαθών (Identify Information Asset Containers): Σαν περιέκτης ορίζεται το μέρος στο οποίο το πληροφοριακό αγαθό αποθηκεύεται, επεξεργάζεται ή μεταφέρεται. Μπορεί να είναι υλικό, λογισμικό, σύστημα, φυσικό αντικείμενο όπως ένα χαρτί, ή ένας άνθρωπος. Υπάρχουν 3 σημαντικά σημεία που αφορούν στους περιέκτες:

1. Η προστασία του πληροφοριακού αγαθού γίνεται μέσω ελέγχων στον περιέκτη του.
2. Ο βαθμός ασφάλειας του αγαθού εξαρτάται από τον βαθμό ελέγχου του περιέκτη του.
3. Ευπάθειες και απειλές στον περιέκτη μεταβιβάζονται και στο αγαθό.

Επίσης είναι σημαντικό να καθοριστεί αν το αγαθό βρίσκεται σε σημείο που δεν ελέγχεται από τον οργανισμό (π.χ. εξωτερικό συνεργάτη). Στο βήμα αυτό υπάρχει μόνο 1 δραστηριότητα.

1η Δραστηριότητα (Activity 1): Στα Φ.Ε. 9a, 9b, 9c καθορίζονται και καταγράφονται οι περιέκτες ως εξής:

Στο 9a καθορίζονται οι τεχνικοί περιέκτες εσωτερικοί και εξωτερικοί.

Στο 9b καθορίζονται οι φυσικές τοποθεσίες που υπάρχει το αγαθό εσωτερικά ή εξωτερικά του οργανισμού.

Στο 9c καθορίζονται οι άνθρωποι που έχουν λεπτομερή γνώση του αγαθού εσωτερικά ή εξωτερικά του οργανισμού.

Θα πρέπει τα Φ.Ε. να συμπληρωθούν όσο πιο λεπτομερώς γίνεται. Επίσης χρειάζεται συνεργασία με τους ιδιοκτήτες των αγαθών, οπότε θα πρέπει όπου είναι δυνατό οι ιδιοκτήτες να καταγραφούν.

Φάση 3. Καθορισμός Απειλών (Identify Threats)

4ο Βήμα (Step 4). Καθορισμός Επισφαλών Περιοχών (Identify Areas of Concern): Μια περιγραφική έκθεση που εκθέτει με λεπτομέρειες μια κατάσταση του πραγματικού κόσμου η οποία μπορεί να επηρεάσει ένα αγαθό του οργανισμού. Σε αυτό το βήμα δημιουργούνται τα

προφίλ των κινδύνων των αγαθών. Σαν κίνδυνος ορίζεται ο συνδυασμός μιας απειλής και η επίπτωση της διενέργειας της απειλής στο αγαθό. Ο καθορισμός των επισφαλών περιοχών τροφοδοτεί το επόμενο 5ο βήμα όπου δημιουργούνται τα προφίλ των κινδύνων. Στο 4ο βήμα διενεργείται 1 δραστηριότητα.

1η Δραστηριότητα (Activity 1): Χρησιμοποιείται το Φ.Ε. 10. Σημείο αναφοράς αποτελούν τα Φ.Ε. 9a, 9b, 9c. Χρησιμοποιώντας τα φύλλα αυτά:

Επανεξετάζονται οι περιέκτες και επιτελούν την αφετηρία αναζήτησης των επισφαλών περιοχών.

Εγγράφονται οι επισφαλείς περιοχές στο Φ.Ε. 10. Χρησιμοποιείται διαφορετικό φύλλο για κάθε επισφαλή περιοχή.

Επεκτείνονται οι επισφαλείς περιοχές για να δημιουργηθούν σενάρια απειλών. Σενάριο είναι η λεπτομερής καταγραφή των ιδιοτήτων της απειλής. Στο Φ.Ε. 10 εγγράφουμε στις στήλες 1 έως 4 τα παρακάτω:

Δράστης (Actor)

Μέσα - Τρόποι (Means)

Κίνητρο (Motive)

Αποτέλεσμα (Outcome)

Στη στήλη 5 καταγράφεται ο τρόπος με τον οποίο η απειλή μπορεί να επηρεάσει τις απαιτήσεις ασφάλειας που έχουμε καθορίσει για το αγαθό.

Η διαδικασία συνεχίζεται για κάθε περιέκτη που έχουμε καθορίσει. Είναι βασικό να ξέρουμε ότι για κάθε περιέκτη μπορεί να υπάρξουν περισσότερες της 1 επισφαλείς περιοχές.

Σε κάθε Φ.Ε. 10 καταγράφεται ένας κίνδυνος. Οπότε για κάθε αγαθό μπορεί να υπάρξουν περισσότερα του ενός Φ.Ε. 10.

5ο Βήμα (Step 5). Καθορισμός Σεναρίων Απειλών (Identify Threat Scenarios): Στο βήμα αυτό επεκτείνονται οι επισφαλείς περιοχές για να καταγραφούν τα σενάρια απειλών. Μια απειλή έχει τις παρακάτω ιδιότητες:

Αγαθό (Asset): Κάτι με αξία για τον οργανισμό

Πρόσβαση/Μέσο (Access/Means): Αφορά μόνο σε ανθρώπους και είναι ο τρόπος πρόσβασης στο αγαθό.

Δράστης (Actor): Ποιος ή τι μπορεί να παραβιάσει τις απαιτήσεις ασφάλειας του αγαθού, οι οποίες είναι:

- Εμπιστευτικότητα (Confidentiality)
- Ακεραιότητα (Integrity)
- Διαθεσιμότητα (Availability)

Κίνητρο (Motive): Αφορά μόνο σε ανθρώπους και μπορεί για παράδειγμα να είναι:

- Σκόπιμα (Deliberate)
- Τυχαία (Accidental)

Αποτέλεσμα (Outcome): Το αποτέλεσμα της παραβίασης των απαιτήσεων ασφάλειας. Μπορεί να είναι:

- Αποκάλυψη (Disclosure)
- Τροποποίηση (Modification)
- Απώλεια/Καταστροφή (Loss/Destruction)
- Διακοπή (Interruption)

Στο 5ο βήμα ελέγχουμε για σενάρια απειλών τα οποία δεν τα έχουμε εντοπίσει στα προηγούμενα βήματα και διενεργούνται 3 δραστηριότητες.

1η Δραστηριότητα (Activity 1): Χρησιμοποιούνται τα Φ.Ε. 9a, 9b, 9c τα οποία συμπληρώνουμε με τη βοήθεια των ερωτηματολογίων για τα σενάρια απειλών.

2η Δραστηριότητα (Activity 2): Στη δραστηριότητα αυτή ολοκληρώνουμε το Φ.Ε. 10.

3η Δραστηριότητα (Activity 3): Η δραστηριότητα 3 είναι προαιρετική και σε αυτή προσθέτουμε και την πιθανότητα να συμβεί ένα σενάριο απειλής. Στην ποιοτική ανάλυση οι τιμές της πιθανότητας είναι:

Χαμηλή (Low)

Μέτρια (Medium)

Υψηλή (High)

Οι πιθανότητες πρέπει να οριστούν για κάθε καθορισμένη απειλή.

Φάση 4. Καθορισμός και Ελαχιστοποίηση Κινδύνων (Identify and Mitigate Risks)

6ο Βήμα (Step 6). Καθορισμός Κινδύνων (Identify Risks): Στο βήμα αυτό διενεργείται 1 δραστηριότητα στην οποία υπολογίζουμε πως το κάθε σενάριο απειλής που έχουμε καταγράψει στο Φ.Ε. 10, Κίνδυνος Πληροφορικού Αγαθού (Information Asset Risk Worksheet), επηρεάζει τον οργανισμό. Συμπληρώνουμε στο Φ.Ε. 10 το τμήμα 7, με τις συνέπειες από το σενάριο απειλών π.χ.

7ο Βήμα (Step 7). Ανάλυση Κινδύνων (Analyze Risks): Στο βήμα 7 μετρούνται ποιοτικά οι ζημιές που επιφέρει ένας κίνδυνος σε κάθε αγαθό του οργανισμού. Οι μετρήσεις αυτές μας βοηθούν στο να ταξινομήσουμε τους κινδύνους και να καθορίσουμε ποιους θα ελαχιστοποιήσουμε πρώτα.

Πιθανότητα Απειλής (κατάσταση) + Επίπτωση (συνέπεια) = Κίνδυνος

[Βήμα 4 και 5] + [Βήμα 6] = Κίνδυνος

Στο βήμα 7 διενεργούνται 2 δραστηριότητες για κάθε ΦΕ-10.

1η Δραστηριότητα (Activity 1): Ελέγχουμε για σενάρια απειλών τα οποία δεν τα έχουμε εντοπίσει στα προηγούμενα βήματα. Χρησιμοποιούνται τα Φ.Ε. 9a, 9b, 9c τα οποία συμπληρώνουμε με τη βοήθεια των ερωτηματολογίων για τα σενάρια απειλών.

2η Δραστηριότητα (Activity 2): Στη δραστηριότητα αυτή υπολογίζεται στη στήλη του ΦΕ-10 το σχετικό σκορ επικινδυνότητας για την απειλή.

8ο Βήμα (Step 8). Επιλογή Τεχνικών Ελαχιστοποίησης Κινδύνων (Select Mitigation Approach): Στο βήμα αυτό διενεργούνται 3 δραστηριότητες.

1η Δραστηριότητα (Activity 1): Ταξινόμηση των κινδύνων σύμφωνα με τη βαθμολογία κινδύνου.

2η Δραστηριότητα (Activity 2): Καθορισμός ελαχιστοποίησης κινδύνου.

3η Δραστηριότητα (Activity 3): Ορισμός στρατηγικής ελαχιστοποίησης.

Κεφάλαιο 6
Μελέτη Ασφάλειας

Είναι δεδομένο ότι το πληροφοριακό σύστημα ενός οργανισμού ή επιχείρησης είναι μείζονος σημασίας και θα πρέπει να προστατεύεται από κάθε είδους απειλές, χωρίς όμως, η προστασία αυτή να εμποδίζει τη ροή των πληροφοριών. Πολύ περισσότερο το πληροφοριακό σύστημα ενός Νοσοκομείου είναι ζήτημα ζωτικής σημασίας για την απρόσκοπτη λειτουργία του και την παροχή των υπηρεσιών υγείας στους πολίτες. Η παρούσα μεταπτυχιακή διατριβή στοχεύει στην περιγραφή των απαραίτητων διαδικασιών που θα πρέπει να τηρηθούν για την επίτευξη της ασφάλειας του Ολοκληρωμένου Πληροφοριακού Συστήματος του Νοσοκομείου «HOSPITAL».

6.1 Οριοθέτηση Μελέτης

Η Μελέτη Ασφάλειας του ΠΣ του νοσοκομείου «HOSPITAL» αποτελεί μια μεθοδική και ολοκληρωμένη προσέγγιση στην αντιμετώπιση των κινδύνων που αντιμετωπίζει το ΠΣ.

6.1.1 Ορισμοί Βασικών Εννοιών και Συντομογραφίες

Στον πίνακα 6.1 που ακολουθεί ορίζονται οι βασικές έννοιες της ασφάλειας πληροφοριών που θα χρησιμοποιηθούν στη Μελέτη Ασφάλειας και στον πίνακα 6.2 οι συντομογραφίες που υπάρχουν σε αυτή.

Δεδομένα	Data	Ένα σύνολο κατανοητών συμβόλων που έχουν καταγραφεί.
Πληροφορία	Information	Τα δεδομένα μαζί με την έννοια που τους αποδίδεται.
Υπολογιστικό Συγκρότημα	IT Assebly	Συλλογή υπολογιστικού υλικού, λογισμικού, τηλεπικοινωνιακού εξοπλισμού ή άλλων υπολογιστικών εξαρτημάτων που χρησιμοποιείται για τη διαχείριση πληροφοριών.
Υπολογιστικό Σύστημα	IT System	Υπολογιστικό Συγκρότημα εγκατεστημένο σε συγκεκριμένη τοποθεσία, με συγκεκριμένο περιβάλλον που ανταποκρίνεται σε συγκεκριμένο σκοπό.
Πληροφοριακό Σύστημα	Information System	Υπολογιστικό συγκρότημα μαζί με τις πληροφορίες που διαχειρίζεται.
Υπολογιστικός Πόρος	IT Resource	Οτιδήποτε αξιοποιείται από ένα υπολογιστικό σύστημα για να διαχειριστεί πληροφορίες.
Εφαρμογή	Application	Πληροφορίες, λογισμικό και διαδικασίες που έχουν σχεδιαστεί για την επίτευξη συγκεκριμένων στόχων.
Αξία	Value	Σπουδαιότητα εκφραζόμενη σε χρηματικούς ή άλλους όρους.
Αγαθό	Asset	Πληροφορίες, δεδομένα ή υπολογιστικοί πόροι που έχουν αξία.
Ιδιοκτήτης	Owner	Πρόσωπο που κατέχει ή είναι υπεύθυνο για ένα αγαθό και που έχει το δικαίωμα να καθορίσει πως μπορεί να χρησιμοποιηθεί,

		να μεταβληθεί ή να διατεθεί το αγαθό αυτό.
Εξουσιοδότηση	Authorization	Άδεια που παρέχεται από τον ιδιοκτήτη για κάποιο σκοπό.
Χρήστης	User	Πρόσωπο ή διεργασία που χρησιμοποιεί ολόκληρο ή μέρος του πληροφοριακού συστήματος.
Προσπέλαση	Access	Η δυνατότητα μιας οντότητας να αξιοποιεί πληροφορίες ή υπολογιστικούς πόρους, στο πλαίσιο ενός πληροφοριακού συστήματος.
Ιδιότητες αγαθού:	Asset Attributes	Οι ιδιότητες του αγαθού που πρέπει να προστατευτούν.
Ακεραιότητα	Integrity	Αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας
Αυθεντικότητα	Authenticity	Αποφυγή ατελειών και ανακριβειών κατά τη διάρκεια εξουσιοδοτημένων τροποποιήσεων μιας πληροφορίας.
Εγκυρότητα	Validity	Απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας.
Διαθεσιμότητα	Availability	Αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας σε εξουσιοδοτημένους χρήστες.
Εμπιστευτικότητα	Confidentiality	Αποφυγή αποκάλυψης πληροφοριών χωρίς την άδεια του ιδιοκτήτη της.
Ασφάλεια	Security	Προστασία της διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των πληροφοριών.
Ασφάλεια Πληροφοριών	Information Security	Διασφάλιση εμπιστευτικότητας, εγκυρότητας, αυθεντικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών.
Ζημιά	Harm	Ο περιορισμός μιας ή περισσοτέρων ιδιοτήτων των αγαθών που χρήζουν προστασίας.
Ρήγμα Ασφάλειας	Breach of Security	Μη εξουσιοδοτημένη αποκάλυψη, τροποποίηση ή απόκρυψη πληροφοριών.
Παραβίαση	Violation	Γεγονός κατά το οποίο περιορίστηκαν κάποιες από τις αυθεντικότητα, διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα, εγκυρότητα.
Απειλή	Threat	Ότι μπορεί να περιορίσει την ασφάλεια ενός πληροφοριακού συστήματος.

Αδυναμία	Vulnerability	Χαρακτηριστικό ενός πληροφοριακού συστήματος που μπορεί να επιτρέψει να συμβεί μια παραβίαση.
Περιστατικό	Incident	Γεγονός που συνέβη ενδεχομένων εξαιτίας μιας απειλής.

Πίνακας 6.1: Ορισμοί Βασικών Εννοιών

ΟΠΣΥ	Ολοκληρωμένο Πληροφοριακό Σύστημα Υγείας
ΟΠΣΝ	Ολοκληρωμένο Πληροφοριακό Σύστημα Νοσοκομείου
ΥΠε	Υγειονομική Περιφέρεια
ΤΠΟ	Τμήμα Πληροφορικής και Οργάνωσης
ΚΥ	Κέντρο Υγείας
ΠΙ	Περιφερειακό Ιατρείο
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
ISMS	Information Security Management System
ISO	International Organization for Standardization
SEI	Software Engineering Institute
CMU	Carnegie Mellon University
CERT	Computer emergency response team
DoD	US Department of Defense
HIPAA	Health Insurance Portability and Accountability Act
ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
ΣΕΣ	Σχέδιο Επιχειρησιακής Συνέχειας

Πίνακας 6.2: Συντομογραφίες

6.1.2 Σκοπός της Μελέτης

Σκοπός της μελέτης είναι ο καθορισμός των απαιτούμενων μέτρων που πρέπει να λάβει το νοσοκομείου «HOSPITAL» για τη προστασία των πληροφοριακών αγαθών του. Ειδικότερα, θα καθοριστούν τα εξής:

1. Τα αγαθά του «HOSPITAL» που χρήζουν προστασίας, οι κίνδυνοι για τα αγαθά αυτά και οι επιπτώσεις που θα έχει η παραβίαση της ασφάλειας τους .

2. Τα απαραίτητα μέτρα που πρέπει να ληφθούν για την ασφάλεια των αγαθών αυτών. Τα μέτρα που θα οριστούν θα είναι σύμφωνα με την *αρχή της αναλογικότητας,* θα έχουν δηλαδή κόστος ανάλογο με τις απειλές από τις οποίες προστατεύουν, σύμφωνα με το Ν.2472/97.

3. Η πολιτική ασφάλειας των αγαθών σύμφωνα με τις απαιτήσεις της ΑΠΔΠΧ.

4. Σχέδιο Ανάκαμψης από Καταστροφή, όπου θα παρουσιάζονται οι διαδικασίες επαναφοράς της επιχειρησιακής λειτουργίας του νοσοκομείου μετά από καταστροφή.

5. Κώδικας δεοντολογίας για τους υπαλλήλους του νοσοκομείου που δεν τους δεσμεύει το Ιατρικό Απόρρητο, σύμφωνα με τις απαιτήσεις της ΑΠΔΠΧ.

6.1.3 Έκταση και Όρια της Μελέτης

Επειδή το πληροφοριακό σύστημα του «HOSPITAL» αποτελεί Υποσύστημα του Ολοκληρωμένου Πληροφοριακού Συστήματος Υγείας της Ν΄ Υγειονομικής Περιφέρειας, σημαντικό μέρος των διαδικασιών αυτών αφορούν και το δεύτερο. Επίσης αφορούν τις υγειονομικές δομές που ανήκουν στο «HOSPITAL» και είναι τα Κέντρα Υγείας και τα Περιφερειακά Ιατρεία.

Απαραίτητη είναι η αξιολόγηση και η αναθεώρηση της μελέτης αν θα υπάρξουν αλλαγές και τροποποιήσεις στο ΠΣ. Σε κάθε περίπτωση κάθε δύο χρόνια πρέπει να γίνεται επαναξιολόγηση της.

6.1.4 Μεθοδολογία της Μελέτης

Η μεθοδολογία της μελέτης ακολουθεί τα στάδια του ISO/IEC 27001:2005 για την εκπόνηση ενός Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών – ISMS που είναι τα εξής:

1. Ανάλυση της επικινδυνότητας (Risk Analysis) που περιλαμβάνει:

   1.1. Προσδιορισμό και αποτίμηση των αγαθών

1.2. Εκτίμηση της απειλής

1.3. Εκτίμηση της ευπάθειας

1.4. Εκτίμηση των υφιστάμενων μέτρων προστασίας

1.5. Υπολογισμό της επικινδυνότητας

2. Διαχείριση της επικινδυνότητας (Risk Management) από το οποίο προκύπτει το Σχέδιο Ασφάλειας, το βασικό εργαλείο διαχείρισης της επικινδυνότητας και περιλαμβάνει:

2.1. Επιλογή αντιμέτρων

2.2. Καθορισμός πολιτικής ασφάλειας

2.3. Σύνταξη σχεδίου ασφάλειας

2.4. Εφαρμογή και παρακολούθηση του σχεδίου ασφάλειας

3. Σχέδιο ανάκαμψης από καταστροφή (Disaster Recovery Plan) που περιλαμβάνει τις διαδικασίες που πρέπει να γίνουν αν παρουσιαστεί ένα περιστατικό παραβίασης της ασφάλειας

Για την ανάλυση και διαχείριση της επικινδυνότητας χρησιμοποιήθηκε η τελευταία εξέλιξη της μεθόδου Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), η OCTAVE Allegro.

OCTAVE Allegro

Η μέθοδος OCTAVE αναπτύχθηκε από την ομάδα CERT στο ινστιτούτο SEI του πανεπιστημίου CMU με σκοπό τη δημιουργία μιας μεθόδου που να συμμορφώνεται στις απαιτήσεις για ασφάλεια και ιδιωτικότητα του νόμου HIPAA. Η παραλλαγή OCTAVE Allegro παρουσιάστηκε τον Ιούνιο του 2007. Οι διαδικασίες που καθορίζονται από την μέθοδο είναι σύμφωνες και με το πρότυπο ISO 27001:2005.

Τρεις είναι οι βασικοί λόγοι χρήσης της μεθόδου από το ΤΠΟ για την εκπόνηση της ανάλυσης και της διαχείρισης της επικινδυνότητας. Ο πρώτος λόγος είναι ότι η μέθοδος είναι δωρεάν και μπορεί οποιοσδήποτε να τη χρησιμοποιήσει, οπότε το «HOSPITAL» δεν επιβαρύνεται με επιπλέον κόστη. Ο δεύτερος λόγος είναι ότι η μέθοδος είναι προσανατολισμένη έτσι ώστε να είναι δυνατή η χρήση της από το προσωπικό του κάθε οργανισμού ακόμα και αν δεν είναι εξειδικευμένο στην ανάλυση και διαχείριση επικινδυνότητας. Και ο τρίτος λόγος είναι ότι σε αντίθεση με άλλες μεθόδους και με τις προγενέστερες OCTAVE μεθόδους μπορεί να εφαρμοστεί χωρίς να είναι απαραίτητη η εκτεταμένη εμπλοκή προσωπικού του νοσοκομείου, γεγονός πολύ σημαντικό στα δημόσια νοσοκομεία όπου υπάρχει μεγάλος φόρτος εργασίας και ελλείψεις σε προσωπικό.

Απαιτείται βέβαια η καλή γνώση του ΟΠΣΝ και των διαδικασιών του «HOSPITAL» από το προσωπικό που θα εκπονήσει τη μελέτη, η οποία είναι δεδομένη για τους υπαλλήλους του ΤΠΟ.

Κεφάλαιο 7
Ανάλυση Επικινδυνότητας

Η ανάλυση επικινδυνότητας είναι το πρώτο στάδιο για την Μελέτη Ασφάλειας ενός ΠΣ.

7.1 Σκοπός της Ανάλυση Επικινδυνότητας

Ο κύριος στόχος της Ανάλυσης Επικινδυνότητας είναι εκτίμηση της Επικινδυνότητας των Αγαθών του ΠΣ του νοσοκομείου. Αφού εκτιμηθεί το επίπεδο επικινδυνότητας στο στάδιο της διαχείρισης της επικινδυνότητας θα οριστούν τα απαιτούμενα μέτρα για τη διαχείριση των απειλών.

7.2 Εύρος της Ανάλυσης Επικινδυνότητας

Η Ανάλυση Επικινδυνότητας αφορά τα πληροφοριακά αγαθά του ΟΠΣΝ του «HOSPITAL» και των ΚΥ και ΠΙ που ανήκουν διοικητικά σε αυτό. Ένα μεγάλο μέρος της υλοποίησης του ΟΠΣΝ έχει γίνει κεντρικοποιημένα από την ΥΠε με αποτέλεσμα να υπάρχουν κοινά αγαθά μεταξύ του «HOSPITAL», των υπολοίπων νοσοκομείων που ανήκουν στην ΥΠε και της διοίκησης της ΥΠε.

Η Ανάλυση Επικινδυνότητας θα πρέπει να επαναξιολογείται και να αναθεωρείται αν υπάρξουν αλλαγές και τροποποιήσεις στο ΠΣ.

7.3 Μεθοδολογία της Ανάλυσης Επικινδυνότητας

Η μέθοδος Ανάλυσης της Επικινδυνότητας που θα ακολουθηθεί είναι η OCTAVE ALLEGRO. Στο πρώτο βήμα της μεθόδου θα γίνει ο προσδιορισμός των κρίσιμων αγαθών του ΠΣ. Για τον προσδιορισμό αυτό χρησιμοποιήθηκε η υπάρχουσα τεκμηρίωση των υποσυστημάτων του ΠΣ, η οποία έχει δοθεί από τους εξωτερικούς συνεργάτες που τα υλοποίησαν σε συνδυασμό με τις γνώσεις των υπαλλήλων του ΤΠΟ για το ΠΣ.

Ο προσδιορισμός της επικινδυνότητας των αγαθών είναι συνάρτηση τριών παραγόντων.

1. Των **απειλών** για ένα αγαθό. Οι απειλές για τα αγαθά κατηγοριοποιούνται σε
    1.1. Σκόπιμες όπως:
        1.1.1. Κλοπή υλικού
        1.1.2. Καταστροφή υλικού
        1.1.3. Μη εξουσιοδοτημένη χρήση του ΠΣ
        1.1.4. Εισαγωγή κακόβουλου λογισμικού
        1.1.5. Κατάχρηση πόρων
    1.2. Ακούσιες όπως:
        1.2.1. Φυσικές Καταστροφές

1.2.1.1. Πλημμύρα

1.2.1.2. Πυρκαγιά

1.2.2. Διακοπή παροχής ηλεκτρικής ενέργειας

1.2.3. Αστοχία υλικού ή λογισμικού

1.2.4. Λάθη εξουσιοδοτημένων χρηστών

2. Της **αδυναμίας** (ευπάθειας) στην ασφάλεια του αγαθού. Η Ανάλυση της Επικινδυνότητας για το «HOSPITAL» θα γίνει θεωρώντας ότι για κανένα αγαθό δεν έχουν ληφθεί μέτρα ασφάλειας.

3. Της **επίπτωσης** που θα έχει για το νοσοκομείο ένα περιστατικό ασφάλειας που θα επηρεάσει μια από τις ιδιότητες των πληροφορικών αγαθών, την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα. Θα εξετασθούν δηλαδή, οι επιπτώσεις για περιστατικά ασφάλειας που μπορεί να οδηγήσουν σε:

   3.1. Αποκάλυψη δεδομένων σε μη εξουσιοδοτημένα άτομα (εμπιστευτικότητα).

   3.2. Τροποποίηση δεδομένων (ακεραιότητα) από μη εξουσιοδοτημένα άτομα ή λανθασμένα από εξουσιοδοτημένους χρήστες.

   3.3. Διακοπή εργασιών (διαθεσιμότητα)

   3.4. Καταστροφή αγαθών (διαθεσιμότητα)

   Σε κάθε περίπτωση η εκτίμηση θα γίνεται λαμβάνοντας υπόψη το χειρότερο σενάριο. Η επίπτωση θα εκτιμάται στην παρακάτω κλίμακα:

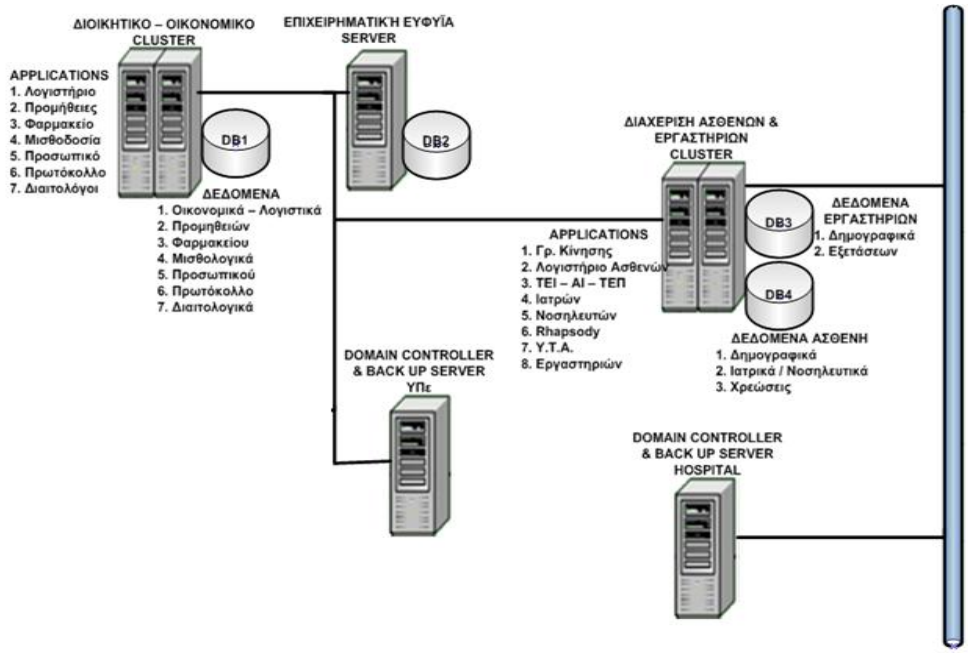
   1. Χαμηλή με βαθμό 1
   2. Μέτρια με βαθμό 2
   3. Υψηλή με βαθμό 3

4. Της **πιθανότητας** να συμβεί το περιστατικό ασφάλειας. Και η πιθανότητα θα εκτιμάται στην κλίμακα:

   1. Χαμηλή με βαθμό 1
   2. Μέτρια με βαθμό 2
   3. Υψηλή με βαθμό 3

7.4 Αγαθά του ΠΣ

Στην σχήμα 7.1 παρουσιάζεται μια συνολική απεικόνιση των αγαθών που βρίσκονται στο δωμάτιο εξυπηρετητών του νοσοκομείου και αποτελούν το βασικό εξοπλισμό υλοποίησης των ΟΠΣΥ - ΟΠΣΝ.



Σχήμα 7.1: Αγαθά Δωματίου Εξυπηρετητών

Το σύνολο των αγαθών του ΟΠΣΝ – όχι μόνο του δωματίου εξυπηρετητών - ομαδοποιείται στις παρακάτω κατηγορίες:

1. ΔΕΔΟΜΕΝΑ

1.1. Δημογραφικά Δεδομένα Ασθενή
1.2. Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή
  1.2.1. Δεδομένα Φαρμακείου (Συνταγολόγια, παραγγελία υλικού κλπ)
  1.2.2. Δεδομένα Εργαστηρίων (Παραγγελία εξετάσεων, Αποτελέσματα)
  1.2.3. Δεδομένα Νοσηλείας (Ασθένεια, έκβαση κλπ)
  1.2.4. Δεδομένα Χρεώσεων Ασθενή – Ταμείου Ασθενή
1.3. Δεδομένα Ραντεβού Ασθενή
1.4. Δεδομένα του Προσωπικού του Νοσοκομείου
  1.4.1. Μισθολογικά δεδομένα
  1.4.2. Υπηρεσιακά δεδομένα
1.5. Οικονομικά – Λογιστικά δεδομένα

1.6. Δεδομένα Προμηθειών

1.6.1.Δεδομένα Αποθηκών

1.6.2.Δεδομένα Φαρμακείου

1.7. Δεδομένα Κεντρικής Γραμματείας – Πρωτόκολλο

1.8. Δεδομένα Αντιγράφων Ασφάλειας

2. ΥΠΟΣΥΣΤΗΜΑΤΑ - ΕΦΑΡΜΟΓΕΣ

2.1. Υποσύστημα Γρ. Κίνησης

2.2. Υποσύστημα Γρ. Εξωτερικών Ιατρείων – Απογευματινών Ιατρείων

2.3. Υποσύστημα Επειγόντων Περιστατικών

2.4. Υποσύστημα Κλινικής / Ορόφου

2.5. Υποσύστημα Λογιστηρίου Ασθενών

2.6. Υποσύστημα Φαρμακείου

2.7. Υποσύστημα Διαιτολόγων

2.8. Υποσύστημα Εργαστηρίων

2.9. Υποσύστημα Ταυτοποίησης Ασθενών

2.10. Υποσύστημα Διοικητικού – Οικονομικού

2.11. Υποσύστημα Προμηθειών

2.12. Υποσύστημα Διαχείρισης Προσωπικού - Μισθοδοσίας

2.13. Υποσύστημα Κεντρικής Γραμματείας - Πρωτόκολλο

2.14. Υποσύστημα Επιχειρηματική Ευφυΐας

2.15. Σύστημα Ηλεκτρονικής συνταγογράφησης / Παραγγελίας εξετάσεων

2.16. Υποσύστημα Ραντεβού των ασθενών

3. ΥΛΙΚΟ (HARDWARE)

3.1. Συστοιχία (cluster) 2 servers για Διοικητικό – Οικονομικό ΠΚΔ

3.2. 1 Server για Υπηρεσίες Domain Controller και Back up ΠΚΔ

3.3. Σύστημα Back Up ΠΚΔ

3.4. Συστοιχία (cluster) 2 servers για Διαχείριση Ασθενών – Εργαστήρια ΚΔΝ

3.5. 1 Server για Υπηρεσίες Domain Controller και Back up ΚΔΝ

3.6. Σύστημα Back Up ΚΔΝ

3.7. Υποδομή Δικτύου ΚΔΝ

3.8. Σταθμοί Εργασίας HOSPITAL

3.9. ADSL Σύνδεση Π.Ι.

3.10. Σταθμοί Εργασίας Π.Ι.

4. Γ. ΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ

4.1. Τέσσερις (4) Βάσεις δεδομένων Microsoft SQL 2000

Η μέθοδος OCTAVE Allegro επικεντρώνεται καταρχήν στα δεδομένα του ΠΣ. Αφού θα εκτιμηθούν οι κίνδυνοι για τα δεδομένα, ορίζουμε τι μέτρα προστασίας θα χρησιμοποιηθούν για την προστασία των περιεκτών των δεδομένων. Για την διαδικασία εκτίμησης των κινδύνων τα δεδομένα του ΟΠΣΝ, θα ομαδοποιηθούν ανάλογα με το είδος τους και το Υποσύστημα που τα διαχειρίζεται. Οι ομάδες των δεδομένων είναι :

1. Δημογραφικά Δεδομένα Ασθενή
2. Ιατρικά / Νοσηλευτικά Δεδομένα τα οποία περιλαμβάνουν:
   2.1. Ιατρικά δεδομένα
   2.2. Δεδομένα νοσηλείας
   2.3. Εργαστηριακά δεδομένα
   2.4. Διαιτολογικά δεδομένα
   2.5. Δεδομένα του Φαρμακείου σχετικά με τα συνταγολόγια των ασθενών
3. Δεδομένα του προσωπικού του νοσοκομείου
4. Δεδομένα Ραντεβού του Ασθενή στα ΕΙ και ΑΙ
5. Οικονομικά – Λογιστικά δεδομένα
6. Δεδομένα Προμηθειών που περιλαμβάνουν δεδομένα του Υλικού, των Αποθηκών αλλά και της Αποθήκης του Φαρμακείου
7. Δεδομένα της Κεντρικής Γραμματείας, το Πρωτόκολλο.
8. Δεδομένα Εξυπηρετητή

7.5 Αποτίμηση κινδύνων

Για την αποτίμηση της επίπτωσης των κινδύνων στα αγαθά, στο OCTAVE Allegro τα πέντε (5) Πεδία Επιπτώσεων βαθμολογούνται και ταξινομούνται ανάλογα με την αξία τους για το νοσοκομείο. Το πιο κρίσιμο έχει βαθμό 5. Για το «HOSPITAL», έχουν ως εξής:

1. Φήμη και Εμπιστοσύνη πελατών → **4**
2. Οικονομικά → **2**
3. Παραγωγικότητα → **3**
4. Ασφάλεια και Υγεία → **5**
5. Πρόστιμα και Νομικές Κυρώσεις → **1**

Για καθένα αγαθό καταγράφεται η αξιολόγηση της επίπτωσης σε καθένα από τα Πεδία Επιπτώσεων, αν από την απειλή προκληθεί Αποκάλυψη σε μη εξουσιοδοτημένα άτομα, Μη εξουσιοδοτημένη Τροποποίηση, Διακοπή διαθεσιμότητας, Καταστροφή.

Στον Πίνακα 7.1 καταγράφεται η αξιολόγηση της επίπτωσης σε καθένα από τα Πεδία Επιπτώσεων από την απειλή. Για ευκολία στη διαχείριση αντί για κάθε απειλή χωριστά η αξιολόγηση γίνεται σύμφωνα με τις συνέπειες της απειλής στο αγαθό. Στο τέλος της διαδικασίας θα ορίσουμε τις απειλές που προκαλούν τις συνέπειες.

Συνέπεια: Αποκάλυψη σε μη εξουσιοδοτημένα άτομα

ΑΓΑΘΟ		Φήμη (4)	Οικον. (2)	Παραγ. (3)	Ασφ/Υγ (5)	Πρόσ (1)
1	Δημογραφικά Δεδομένα Ασθενή	Υψηλή	Υψηλή	Υψηλή	-	Υψηλή
2	Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή	Υψηλή	Υψηλή	Υψηλή	-	Υψηλή
3	Δεδομένα του Προσωπικού του Νοσοκομείου	Μέτρια	Μέτρια	Μέτρια	-	Υψηλή
4	Δεδομένα Ραντεβού Ασθενή	Μέτρια	-	Χαμηλή	-	Χαμηλή
5	Οικονομικά – Λογιστικά δεδομένα	Χαμηλή	Χαμηλή	Μέτρια	-	Χαμηλή
6	Δεδομένα Προμηθειών	Χαμηλή	Χαμηλή	Μέτρια	-	Χαμηλή
7	Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολ.	-	-	-	-	-
8	Δεδομένα Εξυπηρετητή	Χαμηλή	-	-	-	-

Συνέπεια: Τροποποίηση των δεδομένων

ΑΓΑΘΟ		Φήμη (4)	Οικον. (2)	Παραγ. (3)	Ασφ/Υγ (5)	Πρόσ (1)
1	Δημογραφικά Δεδομένα Ασθενή	Μέτρια	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
2	Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή	Μέτρια	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
3	Δεδομένα του Προσωπικού του Νοσοκομείου	Μέτρια	Χαμηλή	Μέτρια	Χαμηλή	Χαμηλή
4	Δεδομένα Ραντεβού Ασθενή	Μέτρια	Χαμηλή	Χαμηλή	-	Χαμηλή
5	Οικονομικά – Λογιστικά δεδομένα	Χαμηλή	Μέτρια	Μέτρια	-	Χαμηλή
6	Δεδομένα Προμηθειών	Χαμηλή	Χαμηλή	Μέτρια	-	Χαμηλή
7	Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολ.	-	Χαμηλή	-	-	-
8	Δεδομένα Εξυπηρετητή	-	-	Χαμηλή	-	-

Συνέπεια: Προσωρινή Διακοπή διαθεσιμότητας

ΑΓΑΘΟ	Φήμη	Οικον.	Παραγ.	Ασφ/Υγ	Πρόσ

		(4)	(2)	(3)	(5)	(1)
1	Δημογραφικά Δεδομένα Ασθενή	Μέτρια	Χαμηλή	Υψηλή	-	Χαμηλή
2	Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή	Μέτρια	Χαμηλή	Υψηλή	Χαμηλή	Χαμηλή
3	Δεδομένα του Προσωπικού του Νοσοκομείου	Χαμηλή	Χαμηλή	Μέτρια	-	Χαμηλή
4	Δεδομένα Ραντεβού Ασθενή	Μέτρια	-	Χαμηλή	-	-
5	Οικονομικά – Λογιστικά δεδομένα	Χαμηλή	Χαμηλή	Μέτρια	-	Χαμηλή
6	Δεδομένα Προμηθειών	Χαμηλή	Χαμηλή	Μέτρια	-	-
7	Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολ.	-	-	Μέτρια	-	-
8	Δεδομένα Εξυπηρετητή	Χαμηλή	Χαμηλή	Μέτρια	-	-

Συνέπεια: Καταστροφή και Μόνιμη Διακοπή διαθεσιμότητας

ΑΓΑΘΟ		Φήμη (4)	Οικον. (2)	Παραγ. (3)	Ασφ/Υγ (5)	Πρόσ (1)
1	Δημογραφικά Δεδομένα Ασθενή	Υψηλή	Χαμηλή	Μέτρια	Χαμηλή	Χαμηλή
2	Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή	Υψηλή	Χαμηλή	Υψηλή	Χαμηλή	Μέτρια
3	Δεδομένα του Προσωπικού του Νοσοκομείου	Υψηλή	Χαμηλή	Μέτρια	-	Χαμηλή
4	Δεδομένα Ραντεβού Ασθενή	-	-	Χαμηλή	-	-
5	Οικονομικά – Λογιστικά δεδομένα	Χαμηλή	Υψηλή	Υψηλή	-	Χαμηλή
6	Δεδομένα Προμηθειών	Μέτρια	Μέτρια	Υψηλή	-	Χαμηλή
7	Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολ.	Χαμηλή	-	Μέτρια	-	-
8	Δεδομένα Εξυπηρετητή	Χαμηλή	Μέτρια	Υψηλή	Χαμηλή	-

Πίνακας 7.3: Αξιολόγηση Επιπτώσεων ανά Πεδίο Επιπτώσεων

Η κλίμακα ταξινόμησης της επίπτωσης, Υψηλή, Μέτρια, Χαμηλή βαθμολογείται ως εξής:

- Υψηλή →**3**
- Μέτρια →**2**
- Χαμηλή→**1**

Για κάθε αγαθό υπολογίζεται μια βαθμολογία που είναι το άθροισμα των γινομένων των τιμών των: **Βαθμός Πεδίου Επίπτωσης Χ Βαθμός Επίπτωσης**. Έτσι για κάθε αγαθό και ανάλογα με τις συνέπειες που έχει η πραγματοποίηση μιας απειλής για αυτό, προκύπτει μια βαθμολογία, η οποία είναι αυτή του Πίνακα 7.4 παρακάτω.

Συνέπεια: Αποκάλυψη σε μη εξουσιοδοτημένα άτομα

	ΑΓΑΘΟ	ΒΑΘΜΟΣ
1	Δημογραφικά Δεδομένα Ασθενή	**30**
2	Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή	**30**
3	Δεδομένα του Προσωπικού του Νοσοκομείου	**21**
4	Δεδομένα Ραντεβού Ασθενή	**12**
5	Οικονομικά – Λογιστικά δεδομένα	**13**
6	Δεδομένα Προμηθειών	**13**
7	Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολλο	**0**

Συνέπεια: Τροποποίηση των δεδομένων

	ΑΓΑΘΟ	ΒΑΘΜΟΣ
1	Δημογραφικά Δεδομένα Ασθενή	**19**
2	Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή	**19**
3	Δεδομένα του Προσωπικού του Νοσοκομείου	**22**
4	Δεδομένα Ραντεβού Ασθενή	**19**
5	Οικονομικά – Λογιστικά δεδομένα	**15**
6	Δεδομένα Προμηθειών	**13**
7	Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολλο	**2**

Συνέπεια: Προσωρινή Διακοπή διαθεσιμότητας

	ΑΓΑΘΟ	ΒΑΘΜΟΣ
1	Δημογραφικά Δεδομένα Ασθενή	**20**
2	Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή	**25**
3	Δεδομένα του Προσωπικού του Νοσοκομείου	**13**
4	Δεδομένα Ραντεβού Ασθενή	**11**
5	Οικονομικά – Λογιστικά δεδομένα	**13**
6	Δεδομένα Προμηθειών	**12**
7	Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολλο	**6**

Συνέπεια: Καταστροφή και Μόνιμη Διακοπή διαθεσιμότητας

	ΑΓΑΘΟ	ΒΑΘΜΟΣ
1	Δημογραφικά Δεδομένα Ασθενή	**26**
2	Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή	**30**
3	Δεδομένα του Προσωπικού του Νοσοκομείου	**21**
4	Δεδομένα Ραντεβού Ασθενή	**3**
5	Οικονομικά – Λογιστικά δεδομένα	**20**
6	Δεδομένα Προμηθειών	**22**
7	Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολλο	**10**

Πίνακας 7.4: Συνολική Βαθμολόγηση Επιπτώσεων

Η λίστα των απειλών ταξινομείται σύμφωνα με το βαθμό της επίπτωσης (Πίνακας 7.5).

Απειλή που επιφέρει	Στα Αγαθά	Βαθμός
ΑΠΟΚΑΛΥΨΗ	Δημογραφικά Δεδομένα Ασθενή	30
ΑΠΟΚΑΛΥΨΗ	Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή	30

ΚΑΤΑΣΤΡΟΦΗ	Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή	30
ΚΑΤΑΣΤΡΟΦΗ	Δημογραφικά Δεδομένα Ασθενή	26
ΔΙΑΚΟΠΗ	Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή	25
ΚΑΤΑΣΤΡΟΦΗ	Δεδομένα Προμηθειών	22
ΚΑΤΑΣΤΡΟΦΗ	Δεδομένα Εξυπηρετητή	22
ΤΡΟΠΟΠΟΙΗΣΗ	Δεδομένα του Προσωπικού του Νοσοκομείου	21
ΚΑΤΑΣΤΡΟΦΗ	Δεδομένα του Προσωπικού του Νοσοκομείου	21
ΑΠΟΚΑΛΥΨΗ	Δεδομένα του Προσωπικού του Νοσοκομείου	21
ΔΙΑΚΟΠΗ	Δημογραφικά Δεδομένα Ασθενή	20
ΚΑΤΑΣΤΡΟΦΗ	Οικονομικά – Λογιστικά δεδομένα	20
ΤΡΟΠΟΠΟΙΗΣΗ	Δημογραφικά Δεδομένα Ασθενή	19
ΤΡΟΠΟΠΟΙΗΣΗ	Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή	19
ΤΡΟΠΟΠΟΙΗΣΗ	Δεδομένα Ραντεβού Ασθενή	19
ΤΡΟΠΟΠΟΙΗΣΗ	Οικονομικά – Λογιστικά δεδομένα	15
ΑΠΟΚΑΛΥΨΗ	Οικονομικά – Λογιστικά δεδομένα	13
ΑΠΟΚΑΛΥΨΗ	Δεδομένα Προμηθειών	13
ΤΡΟΠΟΠΟΙΗΣΗ	Δεδομένα Προμηθειών	13
ΔΙΑΚΟΠΗ	Δεδομένα του Προσωπικού του Νοσοκομείου	13
ΔΙΑΚΟΠΗ	Οικονομικά – Λογιστικά δεδομένα	13
ΑΠΟΚΑΛΥΨΗ	Δεδομένα Ραντεβού Ασθενή	12
ΔΙΑΚΟΠΗ	Δεδομένα Προμηθειών	12
ΔΙΑΚΟΠΗ	Δεδομένα Εξυπηρετητή	12
ΔΙΑΚΟΠΗ	Δεδομένα Ραντεβού Ασθενή	11
ΚΑΤΑΣΤΡΟΦΗ	Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολ.	10
ΔΙΑΚΟΠΗ	Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολ.	6
ΑΠΟΚΑΛΥΨΗ	Δεδομένα Εξυπηρετητή	4
ΚΑΤΑΣΤΡΟΦΗ	Δεδομένα Ραντεβού Ασθενή	3
ΤΡΟΠΟΠΟΙΗΣΗ	Δεδομένα Εξυπηρετητή	3
ΤΡΟΠΟΠΟΙΗΣΗ	Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολ.	2
ΑΠΟΚΑΛΥΨΗ	Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολ.	0

Πίνακας 7.5: Ταξινόμηση Επιπτώσεων

Οι απειλές που αντιμετωπίζει το ΠΣ του νοσοκομείου και η πιθανότητα να συμβούν είναι οι εξής:

ΑΠΕΙΛΗ	**ΠΙΘΑΝΟΤΗΤΑ**
Εισαγωγή κακόβουλου κώδικα και ιομορφικού λογισμικού	Υψηλή
Μη εξουσιοδοτημένη χρήση εφαρμογών	Μέτρια
Πλαστή χρήση ταυτότητας νόμιμου χρήστη	Υψηλή
Κατάχρηση πόρων	Υψηλή
Παρακολούθηση επικοινωνιών και υποκλοπή	Χαμηλή
Διείσδυση στο δίκτυο τρίτων	Χαμηλή
Κλοπή πληροφοριών	Υψηλή
Κλοπή υλικού	Μέτρια
Σφάλματα στη χρήση εφαρμογών	Υψηλή

Αστοχία υλικού	Υψηλή
Αστοχία Δικτύου	Μέτρια
Αστοχία λογισμικού	Μέτρια
Απώλεια παροχής ηλεκτρικής ενέργειας	Υψηλή
Φυσικές καταστροφές (φωτιά, πλημμύρα κλπ)	Χαμηλή
Βλάβη στα κλιματιστικά	Μέτρια

Πίνακας 7.6: Απειλές για το ΠΣ

Οι απειλές ταξινομούνται σύμφωνα με τη βαθμολογία τους και την πιθανότητα να συμβούν και χωρίζονται σε τέσσερις ομάδες επικινδυνότητας ως εξής:

Πιθανότητα	**Βαθμολογία**		
	30 to 45	**16 to 29**	**0 to 15**
Υψηλή	ΟΜΑΔΑ 1	ΟΜΑΔΑ 2	ΟΜΑΔΑ 2
Μέτρια	ΟΜΑΔΑ 2	ΟΜΑΔΑ 2	ΟΜΑΔΑ 3
Χαμηλή	ΟΜΑΔΑ 3	ΟΜΑΔΑ 3	ΟΜΑΔΑ 4

Πίνακας 7.7: Ομάδες Απειλών

Έτσι για τα κρίσιμα αγαθά του νοσοκομείου έχουμε την ομαδοποίησή τους όπως φαίνεται στον παρακάτω πίνακα 7.8.

ΑΠΕΙΛΗ	**ΠΙΘ.**	Αγαθό: **Δημογραφικά Δεδομένα Ασθενή**			
		Αποκ	**Τροπ**	**Διακ**	**Κατασ**
		30	**19**	**20**	**26**
Εισαγωγή κακόβουλου κώδικα και ιομορφικού λογισμικού	Υψηλή		2	2	2
Μη εξουσιοδοτημένη χρήση εφαρμογών	Μέτρια		2	2	
Κατάχρηση πόρων	Υψηλή			2	2
Παρακολούθηση επικοινωνιών και υποκλοπή	Χαμηλή	3			
Διείσδυση στο δίκτυο τρίτων	Χαμηλή	3	3	3	3
Κλοπή πληροφοριών	Υψηλή	1			
Κλοπή υλικού	Μέτρια			2	2
Σκόπιμη βλάβη στο υλικό	Χαμηλή			3	3
Σφάλματα στη χρήση εφαρμογών	Υψηλή		2	2	
Αστοχία υλικού	Υψηλή			2	
Αστοχία Δικτύου	Μέτρια			2	
Αστοχία λογισμικού	Μέτρια			2	

Απώλεια παροχής ηλεκτρικής ενέργειας	Υψηλή			2	
Φυσικές καταστροφές (φωτιά, πλημμύρα κλπ)	Χαμηλή				3
Βλάβη στα κλιματιστικά	Υψηλή			2	2

ΑΠΕΙΛΗ	**ΠΙΘ.**	Αγαθό: **Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή**			
		Αποκ	**Τροπ**	**Διακ**	**Κατασ**
		30	**19**	**25**	**30**
Εισαγωγή κακόβουλου κώδικα και ιομορφικού λογισμικού	Υψηλή		2	2	1
Μη εξουσιοδοτημένη χρήση εφαρμογών	Μέτρια		2	2	
Κατάχρηση πόρων	Υψηλή			2	1
Παρακολούθηση επικοινωνιών και υποκλοπή	Χαμηλή	3			
Διείσδυση στο δίκτυο τρίτων	Χαμηλή	3	3	3	2
Κλοπή πληροφοριών	Υψηλή	1			
Κλοπή υλικού	Μέτρια			2	2
Σκόπιμη βλάβη στο υλικό	Χαμηλή			3	3
Σφάλματα στη χρήση εφαρμογών	Υψηλή		2	2	
Αστοχία υλικού	Υψηλή			2	
Αστοχία Δικτύου	Μέτρια			2	
Αστοχία λογισμικού	Μέτρια			2	
Απώλεια παροχής ηλεκτρικής ενέργειας	Υψηλή			2	
Φυσικές καταστροφές (φωτιά, πλημμύρα κλπ)	Χαμηλή				3
Βλάβη στα κλιματιστικά	Υψηλή			2	1

ΑΠΕΙΛΗ	**ΠΙΘ.**	Αγαθό: **Οικονομικά – Λογιστικά δεδομένα**			
		Αποκ	**Τροπ**	**Διακ**	**Κατασ**
		13	**15**	**13**	**20**
Εισαγωγή κακόβουλου κώδικα και ιομορφικού λογισμικού	Υψηλή		2	2	2
Μη εξουσιοδοτημένη χρήση εφαρμογών	Μέτρια		3	3	
Κατάχρηση πόρων	Υψηλή			2	2

Παρακολούθηση επικοινωνιών και υποκλοπή	Χαμηλή	4			
Διείσδυση στο δίκτυο τρίτων	Χαμηλή	4	4	4	3
Κλοπή πληροφοριών	Υψηλή	2			
Κλοπή υλικού	Μέτρια			3	2
Σκόπιμη βλάβη στο υλικό	Χαμηλή			4	3
Σφάλματα στη χρήση εφαρμογών	Υψηλή		2	2	
Αστοχία υλικού	Υψηλή			2	
Αστοχία Δικτύου	Μέτρια			3	
Αστοχία λογισμικού	Μέτρια			3	
Απώλεια παροχής ηλεκτρικής ενέργειας	Υψηλή			2	
Φυσικές καταστροφές (φωτιά, πλημμύρα κλπ)	Χαμηλή				2
Βλάβη στα κλιματιστικά	Υψηλή			2	2

ΑΠΕΙΛΗ	**ΠΙΘ.**	Αγαθό: **Δεδομένα Προμηθειών**			
		Αποκ	**Τροπ**	**Διακ**	**Κατασ**
		13	**13**	**12**	**22**
Εισαγωγή κακόβουλου κώδικα και ιομορφικού λογισμικού	Υψηλή		2	2	2
Μη εξουσιοδοτημένη χρήση εφαρμογών	Μέτρια		3	3	
Κατάχρηση πόρων	Υψηλή			2	2
Παρακολούθηση επικοινωνιών και υποκλοπή	Χαμηλή	4			
Διείσδυση στο δίκτυο τρίτων	Χαμηλή	4	4	4	3
Κλοπή πληροφοριών	Υψηλή	2			
Κλοπή υλικού	Μέτρια			3	2
Σκόπιμη βλάβη στο υλικό	Χαμηλή			4	3
Σφάλματα στη χρήση εφαρμογών	Υψηλή		2	2	
Αστοχία υλικού	Υψηλή			2	
Αστοχία Δικτύου	Μέτρια			3	
Αστοχία λογισμικού	Μέτρια			3	
Απώλεια παροχής ηλεκτρικής ενέργειας	Υψηλή			2	
Φυσικές καταστροφές (φωτιά, πλημμύρα κλπ)	Χαμηλή				2
Βλάβη στα κλιματιστικά	Υψηλή			2	2

ΑΠΕΙΛΗ	**ΠΙΘ.**	Αγαθό: **Δεδομένα Ραντεβού Ασθενή**

		Αποκ	Τροπ	Διακ	Κατασ
		12	**19**	**11**	**3**
Εισαγωγή κακόβουλου κώδικα και ιομορφικού λογισμικού	Υψηλή		2	2	2
Μη εξουσιοδοτημένη χρήση εφαρμογών	Μέτρια		2	3	
Κατάχρηση πόρων	Υψηλή			2	2
Παρακολούθηση επικοινωνιών και υποκλοπή	Χαμηλή	4			
Διείσδυση στο δίκτυο τρίτων	Χαμηλή	4	3	1	1
Κλοπή πληροφοριών	Υψηλή	2			
Κλοπή υλικού	Μέτρια			3	3
Σκόπιμη βλάβη στο υλικό	Χαμηλή			4	4
Σφάλματα στη χρήση εφαρμογών	Υψηλή		2	2	
Αστοχία υλικού	Υψηλή			2	
Αστοχία Δικτύου	Μέτρια			3	
Αστοχία λογισμικού	Μέτρια			3	
Απώλεια παροχής ηλεκτρικής ενέργειας	Υψηλή			2	
Φυσικές καταστροφές (φωτιά, πλημμύρα κλπ)	Χαμηλή				4
Βλάβη στα κλιματιστικά	Υψηλή			2	2

ΑΠΕΙΛΗ	**ΠΙΘ.**	Αγαθό: **Δεδομένα Προσωπικού**			
		Αποκ	**Τροπ**	**Διακ**	**Κατασ**
		21	**21**	**13**	**21**
Εισαγωγή κακόβουλου κώδικα και ιομορφικού λογισμικού	Υψηλή		2	2	2
Μη εξουσιοδοτημένη χρήση εφαρμογών	Μέτρια		2	3	
Κατάχρηση πόρων	Υψηλή			2	2
Παρακολούθηση επικοινωνιών και υποκλοπή	Χαμηλή	3			
Διείσδυση στο δίκτυο τρίτων	Χαμηλή	3	3	1	3
Κλοπή πληροφοριών	Υψηλή	2			
Κλοπή υλικού	Μέτρια			3	2
Σκόπιμη βλάβη στο υλικό	Χαμηλή			4	3
Σφάλματα στη χρήση εφαρμογών	Υψηλή		2	2	
Αστοχία υλικού	Υψηλή			2	
Αστοχία Δικτύου	Μέτρια			3	

Αστοχία λογισμικού	Μέτρια			3	
Απώλεια παροχής ηλεκτρικής ενέργειας	Υψηλή			2	
Φυσικές καταστροφές (φωτιά, πλημμύρα κλπ)	Χαμηλή				3
Βλάβη στα κλιματιστικά	Υψηλή			2	2

ΑΠΕΙΛΗ	**ΠΙΘ.**	Αγαθό: **Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολλο**			
		Αποκ	**Τροπ**	**Διακ**	**Κατασ**
		0	**2**	**6**	**10**
Εισαγωγή κακόβουλου κώδικα και ιομορφικού λογισμικού	Υψηλή		2	2	2
Μη εξουσιοδοτημένη χρήση εφαρμογών	Μέτρια		3	3	
Κατάχρηση πόρων	Υψηλή			2	2
Παρακολούθηση επικοινωνιών και υποκλοπή	Χαμηλή				
Διείσδυση στο δίκτυο τρίτων	Χαμηλή		1	1	1
Κλοπή πληροφοριών	Υψηλή				
Κλοπή υλικού	Μέτρια			3	3
Σκόπιμη βλάβη στο υλικό	Χαμηλή			4	4
Σφάλματα στη χρήση εφαρμογών	Υψηλή		2	2	
Αστοχία υλικού	Υψηλή			2	
Αστοχία Δικτύου	Μέτρια			3	
Αστοχία λογισμικού	Μέτρια			3	
Απώλεια παροχής ηλεκτρικής ενέργειας	Υψηλή			2	
Φυσικές καταστροφές (φωτιά, πλημμύρα κλπ)	Χαμηλή				3
Βλάβη στα κλιματιστικά	Υψηλή			2	2
ΑΠΕΙΛΗ	**ΠΙΘ.**	Αγαθό: **Δεδομένα Εξυπηρετητή**			
		Αποκ	**Τροπ**	**Διακ**	**Κατασ**
		4	**3**	**12**	**22**
Εισαγωγή κακόβουλου κώδικα και ιομορφικού λογισμικού	Υψηλή		2	2	2
Μη εξουσιοδοτημένη χρήση εφαρμογών	Μέτρια		3	3	2
Κατάχρηση πόρων	Υψηλή				

Παρακολούθηση επικοινωνιών και υποκλοπή	Χαμηλή				
Διείσδυση στο δίκτυο τρίτων	Χαμηλή	4	4	4	3
Κλοπή πληροφοριών	Υψηλή	4			
Κλοπή υλικού	Μέτρια			3	2
Σκόπιμη βλάβη στο υλικό	Χαμηλή			4	3
Σφάλματα στη χρήση εφαρμογών	Υψηλή		2	2	2
Αστοχία υλικού	Υψηλή			2	2
Αστοχία Δικτύου	Μέτρια			3	2
Αστοχία λογισμικού	Μέτρια			3	2
Απώλεια παροχής ηλεκτρικής ενέργειας	Υψηλή			2	2
Φυσικές καταστροφές (φωτιά, πλημμύρα κλπ)	Χαμηλή			4	3
Βλάβη στα κλιματιστικά	Υψηλή			2	2

Πίνακας 7.8: Ομαδοποίηση Απειλών

Στον πίνακα 7.8 σε κάθε αγαθό υπάρχει το σχετικό σκορ της επίπτωσης αν εξαιτίας της απειλής συμβεί Αποκάλυψη (Αποκ), Τροποποίηση (Τροπ), Διακοπή (Διακ) και Καταστροφή (Κατασ). Το σκορ αυτό σε συνδυασμό με την πιθανότητα εμφάνισης της απειλής (Χαμηλή, Μέτρια, Υψηλή), εντάσσει την απειλή σε μια ομάδας. Η ομάδα απεικονίζεται με τους αριθμούς 1, 2, 3, 4. Ανάλογα με την ομάδα που ανήκει κάθε απειλή καθορίζουμε τον τρόπο αντιμετώπισής της, ο οποίος μπορεί να είναι:

1. Ελαχιστοποίηση του κινδύνου, όπου λαμβάνονται τα απαραίτητα μέτρα.
2. Αποδοχή του κινδύνου, όπου δεν λαμβάνεται κανένα μέτρο
3. Μεταφορά ευθύνης σε τρίτους, όπως στη περίπτωση ασφάλισης των αγαθών.
4. Αναβολή καθορισμού του τρόπου αντιμετώπισης και επανεκτίμηση

Ο καθορισμός γίνεται ως εξής:

- Ομάδα 1: Ελαχιστοποίηση
- Ομάδα 2: Ελαχιστοποίηση η Αναβολή
- Ομάδα 3: Αναβολή ή Αποδοχή
- Ομάδα 4: Αποδοχή

Η μεταφορά ευθύνης στην παραπάνω κατάταξη εντάσσεται στην ελαχιστοποίηση του κινδύνου.

7.6 Αποτελέσματα Ανάλυσης Επικινδυνότητας

Από την ανάλυση της επικινδυνότητας του «HOSPITAL» προκύπτει ότι οι απειλές με ψηλό βαθμό επικινδυνότητας για τις οποίες θα πρέπει να ληφθούν τα απαραίτητα μέτρα προφύλαξης είναι:

- Μη εξουσιοδοτημένη πρόσβαση σε Εφαρμογές με σκοπό την αποκάλυψη ευαίσθητων προσωπικών ή ιατρικών/νοσηλευτικών δεδομένων.
- Μη εξουσιοδοτημένη πρόσβαση σε Εφαρμογές με σκοπό την τροποποίηση ή καταστροφή ευαίσθητων προσωπικών ή ιατρικών/νοσηλευτικών δεδομένων.
- Μη εξουσιοδοτημένη πρόσβαση απευθείας σε Βάση Δεδομένων με σκοπό την αποκάλυψη ευαίσθητων προσωπικών ή ιατρικών/νοσηλευτικών δεδομένων.
- Μη εξουσιοδοτημένη πρόσβαση απευθείας σε Βάση Δεδομένων με σκοπό την τροποποίηση ή καταστροφή ευαίσθητων προσωπικών ή ιατρικών/νοσηλευτικών δεδομένων.
- Αστοχία υλικού με αποτέλεσμα την μη διαθεσιμότητα των υπηρεσιών στους υπαλλήλους.
- Αστοχία δικτυακού εξοπλισμού με αποτέλεσμα την μη διαθεσιμότητα των υπηρεσιών του δικτύου στους υπαλλήλους.
- Εισαγωγή κακόβουλου κώδικα με αποτέλεσμα την μη διαθεσιμότητα των υπηρεσιών στους υπαλλήλους.
- Σφάλματα στη χρήση των εφαρμογών με αποτέλεσμα λανθασμένη τροποποίηση των δεδομένων.
- Φωτιά ή πλημμύρα με αποτέλεσμα την μη διαθεσιμότητα των υπηρεσιών στους υπαλλήλους.
- Κλοπή υλικού με αποτέλεσμα την μη διαθεσιμότητα των υπηρεσιών στους υπαλλήλους.

Κεφάλαιο 8
Διαχείριση Επικινδυνότητας

Η διαχείριση της επικινδυνότητας είναι το δεύτερο στάδιο για την Μελέτη Ασφάλειας ενός ΠΣ.

8.1 Σκοπός της Διαχείρισης Επικινδυνότητας

Ο κύριος στόχος της Διαχείρισης Επικινδυνότητας είναι να καθορίσει τα απαραίτητα μέτρα που πρέπει να ληφθούν για την προστασία του ΠΣ από τις απειλές.

8.2 Έκταση και Όρια της Διαχείρισης Επικινδυνότητας

Η Διαχείριση Επικινδυνότητας βασίζεται στην Ανάλυση Επικινδυνότητας που έγινε για τα πληροφοριακά αγαθά του ΟΠΣΝ του «HOSPITAL» και των ΚΥ και ΠΙ που ανήκουν διοικητικά σε αυτό.

Σε περιπτώσεις αλλαγών στο ΠΣ και στην Ανάλυση της Επικινδυνότητας, η Διαχείριση Επικινδυνότητας θα πρέπει να επαναξιολογείται και να αναθεωρείται.

8.3 Μεθοδολογία της Διαχείρισης Επικινδυνότητας

Η διαχείριση επικινδυνότητας είναι η διαδικασία καθορισμού του Σχεδίου Ασφάλειας. Τα Σχέδιο Ασφάλειας περιλαμβάνει :

1. Την Πολιτική Ασφάλειας
2. Τα Απαιτούμενα μέτρα

Στη μέθοδο OCTAVE ALLEGRO η βασική παράμετρος για την εκπόνηση των παραπάνω είναι οι Περιέκτες (Containers) της πληροφορίας. Οι Περιέκτες μπορεί να είναι:

- Υλικό: εξυπηρετητές, σταθμοί εργασίας, ο δικτυακός εξοπλισμός
- Λογισμικό: βάσεις δεδομένων, εφαρμογές
- Φυσικά μέσα αποθήκευσης: κασέτες, φάκελοι, έγγραφα
- Κτιριακές εγκαταστάσεις όπου υπάρχουν τα παραπάνω
- Ανθρώπινο δυναμικό με πρόσβαση στο ΟΠΣΝ

Τα μέτρα ασφάλειας είναι κατά βάση τα μέτρα προστασίας των Περιεκτών. Το επίπεδο ασφάλειας των αγαθών είναι το επίπεδο ασφάλειας των Περιεκτών τους. Τα μέτρα τα οποία θα περιγραφούν αναλυτικά παρακάτω, επιγραμματικά ανά περιέκτη είναι (Πίνακας 8.1):

ΠΕΡΙΕΚΤΕΣ	ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ
Δωμάτιο Εξυπηρετητών	Έλεγχος φυσικής πρόσβασης Προστασία από φυσικές καταστροφές Προστασία από φωτιά, πλημμύρα Προστασία από διακοπή ηλεκτροδότησης
Εξυπηρετητές	Έλεγχος πρόσβασης στο λειτουργικό Πρόγραμμα προστασίας από κακόβουλο λογισμικό Αντίγραφα Ασφάλειας Χρήση σύμφωνα με τις οδηγίες του κατασκευαστή Συντήρηση
Βάσεις δεδομένων	Έλεγχος πρόσβασης απευθείας στη βάση Αντίγραφα Ασφάλειας
Δίκτυο	Έλεγχος πρόσβασης Προστασία υλικού από κλοπή Προστασία υλικού από καταστροφή Έλεγχοι διείσδυσης Διαμόρφωση των ρυθμίσεων του ενεργού εξοπλισμού Παρακολούθηση Ανάχωμα Προστασίας
Σταθμοί Εργασίας	Έλεγχος πρόσβασης στο λειτουργικό Συντήρηση Προστασία υλικού από κλοπή, καταστροφή Πρόγραμμα προστασίας από κακόβουλο λογισμικό Χρήση σύμφωνα με τις οδηγίες του κατασκευαστή Ρυθμίσεις USB θυρών, οδηγών DVD
Εφαρμογές	Έλεγχος πρόσβασης Αντίγραφα Ασφάλειας Προστασία από λάθη χρηστών
Κασέτες back up	Προστασία υλικού από κλοπή Διαγραφή δεδομένων σε περίπτωση καταστροφής
Φάκελος Ασθενή	Προστασία από κλοπή (clear desk) Έλεγχος φυσικής πρόσβασης
Έγγραφα	Προστασία από κλοπή (clear desk) Έλεγχος φυσικής πρόσβασης
Υπάλληλοι του νοσοκομείου	Ενημέρωση και ευαισθητοποίηση στην ασφάλεια Κώδικας δεοντολογίας Νομικές κυρώσεις
Διαδίκτυο	Κρυπτογράφηση
Εξωτερικοί συνεργάτες	Συμβόλαια και συμφωνίες για την ασφάλεια

Πίνακας 8.1: Μέτρα προστασίας των περιεκτών

8.4 Πολιτική Ασφάλειας

1. Εισαγωγή

1.1. Ασφάλεια του ΠΣ είναι η προστασία των πληροφοριακών αγαθών του ΠΣ από οποιαδήποτε απειλή μπορεί να προκαλέσει απώλεια μιας από τις ιδιότητες των πληροφοριών:

- Εμπιστευτικότητα
- Διαθεσιμότητα
- Ακεραιότητα

Η πολιτική ασφάλειας καθορίζει τις απαραίτητες διοικητικές κατευθύνσεις και τα μέτρα που πρέπει να ληφθούν, σύμφωνα με τις επιχειρησιακές απαιτήσεις και τη σχετική νομοθεσία για την προστασία της ασφάλειας του ΠΣ.

Η διοίκηση του νοσοκομείου αντιλαμβανόμενη τη σπουδαιότητα της ασφάλειας του ΟΠΣΝ για την επίτευξη της αδιάλειπτης λειτουργίας του για την προσφορά υπηρεσιών υγείας στους πολίτες υποστηρίζει ενεργά και θέτει σε ισχύ την πολιτική ασφάλειας.

2. Στόχοι της Πολιτικής Ασφάλειας

Σκοπός Πολιτικής Ασφάλειας είναι να καθορίσει τα μέτρα και τις κατευθύνσεις που είναι απαραίτητα για την διασφάλιση του ΠΣ του νοσοκομείου. Τα δεδομένα που διαχειρίζεται το νοσοκομείο είναι κυρίως δεδομένα που καλύπτονται από το Ιατρικό Απόρρητο ή δεδομένα προσωπικού χαρακτήρα τα οποία υπόκεινται ειδική νομοθεσία. Επίσης είναι πολύ σημαντικό οι διαδικασίες διαχείρισής τους να γίνονται απρόσκοπτα ώστε το νοσοκομείο να προσφέρει τις υπηρεσίες του στους πολίτες.

Για τη διασφάλιση του ΠΣ η Πολιτική Ασφάλειας ορίζει το πλαίσιο για την επίτευξη των παρακάτω στόχων:

2.1. Επίτευξη του απαραίτητου επίπεδου ασφάλειας του ΟΠΣΝ

2.2. Καθορισμός του πλαισίου διαχείρισης των πληροφοριακών πόρων του ΟΠΣΝ.

2.3. Ενημέρωση και ευαισθητοποίηση των χρηστών σε θέματα ασφάλειας.

2.4. Συμμόρφωση με τη νομοθεσία για την ασφάλεια

3. Εμβέλεια

3.1. Η Πολιτική Ασφάλειας αφορά την ασφαλή διαχείριση των πληροφοριών του ΟΠΣΝ και των πόρων που απαιτούνται για αυτή. Θα εφαρμόζεται από όλο το προσωπικό του νοσοκομείου που μετέχει στη διαχείριση αυτή. Τα απαιτούμενα μέτρα θα τηρούνται και από τους εξωτερικούς συνεργάτες του νοσοκομείου ή τρίτα μέρη που με οποιονδήποτε τρόπο έχουν πρόσβαση τους πόρους του ΟΠΣΝ.

3.2. Η Πολιτική Ασφάλειας θα επανεξετάζεται και θα αναθεωρείται σε περίπτωση αλλαγών ή τροποποιήσεων του ΟΠΣΝ.

4. Καθορισμός ρόλων απαραίτητων για την ασφάλεια του ΟΠΣΝ

Οι παρακάτω ρόλοι πρέπει να καθοριστούν και να ανατεθούν στο προσωπικό, από τη διοίκηση για την υποστήριξη της Πολιτικής Ασφάλειας.

4.1. Υπεύθυνος Ασφάλειας του νοσοκομείου ο οποίος έχει τα εξής καθήκοντα:

- Την τήρηση των μέτρων της Πολιτικής Ασφάλειας από το προσωπικό
- Την διενέργεια προληπτικών ελέγχων για την διαπίστωση αναγκαιότητας λήψης διορθωτικών μέτρων σε σχέση με παρατηρούμενες αδυναμίες ή κενά στους μηχανισμούς ασφάλειας.
- Την εκτέλεση των ενεργειών που απαιτούνται για την πρόληψη, αναγνώριση και αντιμετώπιση απειλών και κινδύνων.
- Το συντονισμό και παρακολούθηση της υλοποίησης των μέτρων για την ελαχιστοποίηση των κινδύνων για την ασφάλεια.
- Επικοινωνία με το προσωπικό για την αντιμετώπιση περιστατικών ασφάλειας.

4.2. Επιτροπή για το Σχέδιο Ανάκαμψης από Καταστροφή

Για τον ορισμό της Επιτροπής θα επιλεγεί ένας υπάλληλος από κάθε νοσοκομείο του ΟΠΣΥ και ένας από τη Διοίκηση της ΥΠε. Η επιτροπή είναι υπεύθυνη για τα εξής:

- Διενέργεια ανάλυσης επικινδυνότητας του ΟΠΣΥ
- Την δημιουργία και ενημέρωση Σχεδίου Ανάκαμψης από Καταστροφές
- Την περιοδική διενέργεια δοκιμών του Σχεδίου Ανάκαμψης από Καταστροφές.
- Την εκκίνηση και υλοποίηση της Ανάκαμψης σε περίπτωση καταστροφής.

4.3. Υπεύθυνος για το Σχέδιο Ανάκαμψης από Καταστροφή

Συμμετέχει στης Επιτροπή για το Σχέδιο Ανάκαμψης από Καταστροφή και είναι υπεύθυνος για τον συντονισμό των εργασιών αυτής.

4.4. Εσωτερικοί χρήστες.

Οι χρήστες του νοσοκομείου, οι οποίοι υποχρεούνται να ακολουθούν την πολιτική ασφάλειας και να ενημερώνουν τον Υπεύθυνο Ασφάλειας για περιστατικά παραβίασης της ασφάλειας.

4.5. Εξωτερικοί χρήστες

Εξωτερικοί συνεργάτες και πάροχοι υπηρεσιών οι οποίοι είναι και αυτοί υποχρεωμένοι στη συμμόρφωση με τα μέτρα της πολιτικής ασφάλειας, μέσω των συμβάσεων ή συμφωνιών που έχουν με το νοσοκομείο.

5. Συμμόρφωση

Όλοι όσοι αποκτούν πρόσβαση στο ΟΠΣΝ – εσωτερικοί και εξωτερικοί χρήστες - έχουν ευθύνη για την ασφάλεια των πληροφοριών και των συστημάτων του. Απαγορεύεται η αποκάλυψη ευαίσθητων προσωπικών δεδομένων ή δεδομένων που καλύπτονται από το Ιατρικό Απόρρητο.

Επίσης απαγορεύονται ενέργειες που μπορεί να προκαλέσουν ζημιά στον εξοπλισμό και πρόβλημα στη διαθεσιμότητα των πληροφοριών.

Η διαχείριση των πληροφοριακών αγαθών θα γίνεται σύμφωνα με την υπάρχουσα νομοθεσία, κανονισμούς ή συμβάσεις με τρίτους .

6. Ασφάλεια εγκαταστάσεων

Για την ασφάλεια των κτιριακών υποδομούν στις οποίες υπάρχει πληροφοριακός εξοπλισμός του ΟΠΣΥ πρέπει να τηρούνται τα εξής μέτρα:

- Ελεγχόμενη πρόσβαση.
- Προστασία από φωτιά, πλημμύρα, φυσικές καταστροφές.
- Προστασία από διακοπή ηλεκτροδότησης.

Ειδικότερα για το δωμάτιο των εξυπηρετητών (Computer Room) θα πρέπει να ισχύουν τα παρακάτω:

- Μόνο το εξουσιοδοτημένο προσωπικό του ΤΠΟ θα έχει πρόσβαση.
- Σε περίπτωση που είναι απαραίτητη η πρόσβαση σε τρίτους, αυτή θα γίνεται υπό την εποπτεία υπαλλήλου του ΤΠΟ.
- Θα υπάρχει σύστημα κλιματισμού
- Θα υπάρχουν συστήματα πυρασφάλειας και πυρόσβεσης.
- Θα ενταχθεί στο σύστημα ηλεκτροδότησης από τη γεννήτρια του νοσοκομείου στην περίπτωση διακοπής ρεύματος.
- Θα υπάρχει σύστημα αδιάλειπτης παροχής ρεύματος για τουλάχιστον 2 ώρες μετά τη διακοπή ρεύματος.
- Ο εξοπλισμός και τα συστήματα προστασίας θα συντηρούνται σύμφωνα με τις προδιαγραφές του κατασκευαστή τους.

7. Ασφάλεια στη χρήση του ΟΠΣΝ

Η χρήση του ΟΠΣΝ θα γίνεται σύμφωνα με την κείμενη νομοθεσία και για τους σκοπούς του νοσοκομείου. Απαγορεύεται η χρήση του ΠΣ με τρόπο που μπορεί να παραβιάζει την Ελληνική ή διεθνή νομοθεσία για την προστασία:

- Δεδομένων προσωπικού χαρακτήρα
- Ιατρικού Απόρρητου
- Πνευματικής Ιδιοκτησίας
- Άλλων νομοθεσιών ή κανονισμών

Στο πλαίσιο αυτό οι χρήστες πρέπει να συμμορφώνονται με τα απαραίτητα μέτρα προστασίας.

7.1. Ασφάλεια Λογισμικού

- Απαγορεύεται η μη εξουσιοδοτημένη πρόσβαση σε εφαρμογές.
- Απαγορεύεται η εγκατάσταση λογισμικού που δεν έχει την απαιτούμενη άδεια χρήσης
- Απαγορεύεται η εγκατάσταση λογισμικού χωρίς την έγκριση του ΤΠΟ
- Απαγορεύεται η τροποποίηση λογισμικού χωρίς την έγκριση του ΤΠΟ
- Η τροποποίηση λογισμικού των υποσυστημάτων του ΟΠΣΥ θα γίνεται πρώτα σε δοκιμαστικό περιβάλλον και μετά θα μπαίνει σε παραγωγική λειτουργία.
- Απαγορεύεται οι χρήστες να εγκαθιστούν προγράμματα από το διαδίκτυο.
- Απαγορεύεται η εκτέλεση προγραμμάτων που λαμβάνονται συνημμένα στο ηλεκτρονικό ταχυδρομείο.
- Στο ΟΠΣΝ θα υπάρχει εγκατεστημένο πρόγραμμα προστασίας από κακόβουλο και ιομορφικό λογισμικό στους εξυπηρετητές και στους σταθμούς εργασίας.
- Σε περίπτωση περιστατικού κακόβουλο λογισμικού ο σταθμός εργασίας θα απομονώνεται και θα καθαρίζεται.
- Θα πρέπει να γίνονται οι απαραίτητες ενημέρωσης του αντιικού λογισμικού.

7.2. Ασφάλεια Εξοπλισμού

- Ο εξοπλισμός του νοσοκομείου καθορίζεται από το ΤΠΟ με την έγκριση της Διοίκησης

- Απαγορεύεται οι χρήστες να χρησιμοποιούν στο δίκτυο του Νοσοκομείου άλλων εξοπλισμό, όπως φορητοί υπολογιστές, πέραν αυτού που έχει εγκαταστήσει το ΤΠΟ.
- Ο εξοπλισμός θα συντηρείται σύμφωνα με τις προδιαγραφές του κατασκευαστή
- Η τεχνική υποστήριξη του εξοπλισμού γίνεται από το ΤΠΟ
- Απαγορεύεται οι χρήστες να επεμβαίνουν, αλλάζουν, τροποποιούν στοιχεία του εξοπλισμού.
- Σε περίπτωση βλάβης θα ενημερώνεται το ΤΠΟ

- Ο εξοπλισμός δεν θα μένει αφύλακτος χωρίς ελεγχόμενη πρόσβαση σε τρίτους.

7.3. Ασφάλεια Δεδομένων

- Τα δεδομένα του νοσοκομείου ταξινομούνται σε 3 ομάδες

— Δημόσια δεδομένα

— Ευαίσθητα προσωπικά δεδομένα που υπόκεινται στο Ν. 2472/97 και στο Ν. 2774/99.

— Ιατρικά δεδομένα που προστατεύονται από το Ιατρικό Απόρρητο.

- Η διαθεσιμότητα των δεδομένων είναι κρίσιμη για τη λειτουργία του Νοσοκομείου
- Απαγορεύεται η αποκάλυψή τους σε μη εξουσιοδοτημένα άτομα
- Απαγορεύεται η μη εξουσιοδοτημένη τροποποίησή τους.

Γι α την προστασία των δεδομένων οι χρήστες πρέπει να τηρούν τα εξής μέτρα:

- Προστασία των συνθηματικών πρόσβασης στο λειτουργικό σύστημα των σταθμών εργασίας
- Προστασία των συνθηματικών πρόσβασης στις λογισμικό εφαρμογών
- Η δομή των συνθηματικών θα είναι τέτοια που θα αποτρέπει την εύκολη αποκάλυψή τους.

— Θα αποτελούνται τουλάχιστον από οκτώ (8) χαρακτήρες

— Θα έχουν τουλάχιστον ένα αριθμό, ένα γράμμα και ένα σύμβολο

- Δεν θα είναι λέξεις που υπάρχουν σε λεξικό
- Θα ελέγχονται αυτοματοποιημένα από εφαρμογή ελέγχου ότι τηρούν την παραπάνω δομή
- Θα αλλάζουν κάθε δύο μήνες
- Θα υπάρχουν διαφορετικά συνθηματικά για το λειτουργικό σύστημα και διαφορετικά για τις εφαρμογές λογισμικού.
- Δεν θα είναι γραμμένα σε εμφανή σημεία
- Στου σταθμούς εργασίας θα είναι ενεργοποιημένη η οθόνη αδράνειας. Σε περίπτωση μη λειτουργίας του σταθμού για χρονικό διάστημα μεγαλύτερο των 15 λεπτών θα ενεργοποιείται. Για να αποκτήσει πρόσβαση ο χρήστης πρέπει να ξαναδώσει τα συνθηματικά του.
- Τα δεδομένα δεν θα στέλνονται μέσω διαδικτύου. Στην περίπτωση που αυτό κριθεί απαραίτητο θα στέλνονται κρυπτογραφημένα.
- Θα παίρνονται εφεδρικά αντίγραφα (back up) ημερήσια, εβδομαδιαία και μηνιαία
- Οι κασέτες του back up θα φυλάσσονται σε ασφαλές μέρος.
- Οι χρήστες έχουν ευθύνη για την προστασία φυσικών μέσων, όπως τον Φάκελο Ασθενή, έγγραφα που περιέχουν δεδομένα που χρήζουν εμπιστευτικότητας.

7.4. Ασφάλεια δικτύου και δικτυακών υπηρεσιών

- Υπεύθυνο για τη διαχείριση του δικτύου είναι το ΤΠΟ
- Η τοπολογία του δικτύου θα είναι καταγραμμένη.
- Πρόσβαση στις υπηρεσίες του δικτύου θα έχουν μόνο εξουσιοδοτημένοι χρήστες.
- Όλες οι συνδέσεις με το διαδίκτυο ή άλλα δίκτυα θα ελέγχονται με αναχώματα ασφάλειας

- Θα υλοποιηθούν ζώνες προστασίας για τα κρίσιμα συστήματα του ΟΠΣΝ, όπως εξυπηρετητές εφαρμογών, εξυπηρετητές συστήματος.

- Θα υλοποιούνται τεχνολογίες ανίχνευσης και προστασίας από εισβολές.

- Η χρήση του Διαδικτύου θα περιορίζεται στην απολύτως αναγκαία για την επίτευξη των εργασιακών στόχων.

- Απαγορεύεται η παράνομη χρήση του διαδικτύου ή του ηλεκτρονικού ταχυδρομείου.

8. Ασφάλεια Πρόσβασης

- Μόνο εξουσιοδοτημένα άτομα θα έχουν πρόσβαση στο ΟΠΣΝ

- Η πρόσβαση θα δίνεται από το ΤΠΟ μετά από έγγραφη αίτηση η οποία έχει εγκριθεί από τη Διοίκηση

- Θα ισχύει η αρχής της «**ελάχιστης πρόσβασης**». Κάθε χρήστης θα έχει πρόσβαση μόνο σε πόρους που είναι απαραίτητοι για την επίτευξη της εργασίας του.

- Θα δημιουργηθούν ρόλοι χρηστών με συγκεκριμένα δικαιώματα για κάθε ρόλο χρήστη.

- Όταν ένας υπάλληλος φύγει ή αλλάξει αντικείμενο εργασίας οι παλιοί του ρόλοι θα απενεργοποιούνται.

- Κάθε χρήστης έχει τόσα δικαιώματα όσα ακριβώς είναι απαραίτητα.

- Θα υπάρχει αρχείο καταγραφής των χρηστών και των ρόλων του καθενός.

- Η πρόσβαση σε όλους τους πόρους του ΟΠΣΝ θα γίνεται με χρήση έγκυρης ταυτότητας χρήστη και κωδικού πρόσβασης.

- Θα ελέγχονται τακτικά τα αρχεία συστήματος με πληροφορίες σύνδεσης των χρηστών, για προσπάθειες μη εξουσιοδοτημένης πρόσβασης.

- Η απομακρυσμένη πρόσβαση τρίτων χρηστών στο ΟΠΣΝ θα γίνεται ελεγχόμενα και θα καταγράφονται:

— Ώρα έναρξης και διακοπής της σύνδεσης

— Διάρκεια της σύνδεσης

— Τα συστήματα στα οποία έγινε η σύνδεση.

9. Διαχείριση Περιστατικών Ασφάλειας

- Θα καθοριστεί διαδικασία αναφοράς περιστατικών παραβίασης της ασφάλειας
- Τα περιστατικά παραβίασης της ασφάλειας θα καταγράφονται σε αρχείο καταγραφής.
- Οι χρήστες θα αναφέρουν τα περιστατικά παραβίασης στον Υπεύθυνο Ασφάλειας ή στο ΤΠΟ
- Τα περιστατικά παραβίασης θα αντιμετωπίζονται άμεσα.
- Θα καταγράφονται στο αρχείο οι διαδικασίες αντιμετώπισης των περιστατικών.

10. Σχέδιο Ανάκαμψης από Καταστροφή

Θα εκπονηθεί Σχέδιο Ανάκαμψης από Καταστροφή που θα καθορίζει τις διαδικασίες για την ανάκαμψη από καταστροφή.

10.1. Το Σχέδιο Ανάκαμψης από Καταστροφή θα είναι καταγεγραμμένο.

10.2. Το Σχέδιο Ανάκαμψης από Καταστροφή θα ελέγχεται και θα επαναξιολογείται αν υπάρξουν τροποποιήσεις και αλλαγές στο ΟΠΣΝ.

10.3. Το Σχέδιο Ανάκαμψης από Καταστροφή θα έχει την έγκριση της Διοίκησης.

10.4. Τα καθήκοντα τήρησής του τα έχουν:

— Ο Υπεύθυνος Ανάκαμψης από Καταστροφή

— Ο Υπεύθυνος Ασφάλειας

— Η ομάδα Ανάκαμψης από Καταστροφή

- Θα υπάρχει συγκεκριμένη διαδικασία για την έναρξη της Ανάκαμψης στην οποία θα ορίζονται τα «**Κριτήρια Ενεργοποίησης**» του Σχεδίου.

- Για την έναρξη της διαδικασία Ανάκαμψης από Καταστροφή πρέπει να δοθεί έγκριση από τον Διοικητή της ΥΠε.

11. Συμμόρφωση με τη νομοθεσία

11.1. Η πολιτική ασφάλειας συμμορφώνεται με τους νόμους και τους κανονισμούς που απορρέουν από:

- Το Ν. 2472/97 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

- Το Ν. 2774/99 για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.

- Το Ιατρικό Απόρρητο

- Τις απαιτήσεις της ΑΠΔΠΧ

    — Σύμφωνα με την απαίτηση της ΑΠΔΠΧ το νοσοκομείο υποχρεούται στη σύνταξη «**Κώδικα Δεοντολογίας**» για τη διαχείριση των δεδομένων που δεν καλύπτονται από το Ιατρικό Απόρρητο. Ο κώδικας δεοντολογίας:

        - Θα εγκριθεί από τη διοίκηση
        - Θα υποβληθεί στην ΑΠΔΠΧ
        - Θα διανεμηθεί στο προσωπικό το οποίο θα δεσμευτεί εγγράφως για την τήρησή του.

Κεφάλαιο 9
Απαιτούμενα Μέτρα

Το δεύτερο βήμα στην εκπόνηση του Σχεδίου Ασφάλειας μετά την Πολιτικής Ασφάλειας είναι ο καθορισμός των απαιτούμενων μέτρων προστασίας.

9.1 Οργάνωση της Ασφάλειας των Πληροφοριών

Το πλαίσιο διαχείρισης για την ασφάλεια των πληροφοριών εντός του οργανισμού.

9.1.1. Εσωτερική Ασφάλεια.

Διαχείριση της Ασφάλειας στο εσωτερικό του οργανισμού.

9.1.1.1. Διοικητικές Υποχρεώσεις.

Η διοίκηση του νοσοκομείου πρέπει να υποστηρίζει ενεργά την εσωτερική ασφάλεια.

9.1.1.1.1. Η διοίκηση πρέπει να εγκρίνει το Σχέδιο Ασφάλειας.

9.1.1.1.2. Πρέπει να οριστεί Υπεύθυνος Ασφάλειας του ΟΠΣΝ.

Ο Υπεύθυνος Ασφάλειας πρέπει να έχει επαρκείς γνώσεις σχετικά με το ΟΠΣΝ και την ασφάλεια πληροφοριών ή να καταρτιστεί για αυτά.

9.2.1.1.3. Πρέπει να οριστεί αντικαταστάτης του Υπεύθυνου Ασφάλειας του ΟΠΣΝ.

Ο αντικαταστάτης του Υπεύθυνου Ασφάλειας του ΟΠΣΝ είναι απαραίτητος στις περιπτώσεις απουσίας του πρώτου.

9.2.1.1.4. Οι αρμοδιότητες του Υπεύθυνου Ασφάλειας του ΟΠΣΝ πρέπει να οριστούν με ακρίβεια και να καταγραφούν.

Οι αρμοδιότητες αυτές περιλαμβάνουν:

- *Διαχείριση του Σχεδίου Ασφάλειας.*
- *Ευθύνη υλοποίησης και εφαρμογής των μέτρων ασφάλειας.*
- *Διεξαγωγή ελέγχων για την εφαρμογή του Σχεδίου Ασφάλειας.*
- *Σύνταξη ετήσιας Έκθεσης Ασφάλειας ΟΠΣ.*

- *Επικοινωνία με τους χρήστες για θέματα ασφάλειας*
- *Διαχείριση περιστατικών ασφάλειας*

9.1.1.2. Συντονισμός Διαδικασιών Ασφάλειας

Οι δραστηριότητες ασφάλειας των πληροφοριών θα πρέπει να είναι συντονισμένες με εκπροσώπους από διάφορα τμήματα του νοσοκομείου.

9.1.1.2.1. Οι διαδικασίες ασφάλειας πρέπει να καταγραφούν και να κοινοποιηθούν στο προσωπικό του νοσοκομείου.

9.1.1.2.2. Η διοίκηση θα πρέπει να φροντίσει για την δέσμευση του προσωπικού στην τήρηση των μέτρων ασφάλειας και του κώδικα δεοντολογίας του νοσοκομείου.

9.1.1.2.3. Η διοίκηση θα πρέπει να ενημερώσει, ευαισθητοποιήσει και εκπαιδεύσει τους χρήστες στα θέματα ασφάλειας.

9.1.1.2.4. Η διοίκηση θα πρέπει να συντονίζει τη διαχείριση εντοπισμένων συμβάντων στην ασφάλεια και την παρακολούθηση και αναθεώρηση των υπαρχόντων μέτρων.

9.1.1.3. Καθορισμός ευθυνών

Όλες οι ευθύνες της ασφάλειας των πληροφοριών θα πρέπει να ορίζονται με σαφήνεια.

9.1.1.3.1. Οι ευθύνες που απορρέουν από την πολιτική ασφάλειας του νοσοκομείου πρέπει να ορίζονται και να κατανέμονται με σαφήνεια στο προσωπικό.

9.1.1.3.2. Τα πληροφορικά αγαθά κάθε υποσυστήματος, οι διαδικασίες ασφάλειας που συνδέονται με αυτά και οι υπεύθυνοι για αυτά, πρέπει να καθορίζονται με σαφήνεια στους χρήστες του υποσυστήματος.

9.1.1.4. Επικοινωνία με τις αρχές

Θα πρέπει να διατηρηθούν οι κατάλληλες επαφές με τις αρμόδιες αρχές.

9.1.1.4.1. Το νοσοκομείο πρέπει να γνωστοποιήσει εγγράφως στην ΑΠΔΠΧ τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας.

9.1.1.4.2. Το νοσοκομείο πρέπει να διατηρεί τις απαιτούμενες από την ΑΠΔΠΧ άδειες λειτουργίας και επεξεργασίας αρχείων.

Οι άδειες είναι:

- Άδεια διοίκησης των υπηρεσιών υγείας

- Άδεια με σκοπό την παροχή υπηρεσιών υγείας

- Άδεια με σκοπό τη διενέργεια μεταγγίσεων αίματος και μεταμόσχευσης οργάνων

- Άδεια με σκοπό τη παροχή υπηρεσιών δημόσιας υγείας

9.1.1.4.3. Το νοσοκομείο πρέπει να ενημερώνει την ΑΠΔΠΧ σχετικά με τις αλλαγές στο ΠΣ και στα μέτρα ασφάλειας.

9.1.1.4.4. Το νοσοκομείο πρέπει να ορίσει διαδικασία αναφοράς περιστατικών παραβίασης της ασφάλειας στις κατάλληλες αρχές.

9.1.2. Ασφάλεια σχετικά με εξωτερικούς συνεργάτες και τρίτους.

Διαχείριση Ασφάλειας σε αγαθά που διαχειρίζονται εξωτερικοί συνεργάτες.

9.1.2.1. Προσδιορισμός κινδύνων σχετικά με τρίτους.

Προσδιορισμός και έλεγχος των κινδύνων που προέρχονται από την επικοινωνία του νοσοκομείου με τρίτους.

9.1.2.1.1. Το νοσοκομείο πρέπει να φροντίζει να υπάρχει συμβόλαιο συντήρησης για τα υποσυστήματα που έχουν αναπτυχθεί από εξωτερικούς συνεργάτες.

9.1.2.1.2. Το νοσοκομείο πρέπει να δεσμεύει τους εξωτερικούς συνεργάτες που έχουν πρόσβαση στα πληροφοριακά αγαθά με συμβάσεις που θα περιέχουν στο ελάχιστο τα εξής:

- Περιγραφή των προσωπικών δεδομένων

- Σκοπό, τόπο και τρόπο επεξεργασίας

- Επίπεδα ασφάλειας και ποιότητας δεδομένων

- Υποχρέωση διατήρησης της εμπιστευτικότητας των πληροφοριών στη διάρκεια της σύμβασης αλλά και μετά τη λήξη της.

- Ρήτρες αναφορικά με παραβιάσεις των όρων της σύμβασης

9.1.2.1.3. Μετά την παράδοση του έργου θα απενεργοποιούνται οι διευκολύνσεις στον εξωτερικό συνεργάτη και θα αλλάζουν τα συνθηματικά που γνωρίζει.

9.1.2.1.4. Οι εργασίες συντήρησης του λογισμικού θα ελέγχονται ως εξής:

- Οι αλλαγές στο λογισμικό θα γίνονται σε δοκιμαστικό περιβάλλον πριν αυτό τεθεί σε παραγωγική λειτουργία

- Οι αλλαγές στο λογισμικό θα ελέγχονται πριν αυτό τεθεί σε παραγωγική λειτουργία.

- Να τηρείται αρχείο συντήρησης του λογισμικού από τον εξωτερικό συνεργάτη.

- Να τηρείται αρχείο συντήρησης του λογισμικού από το νοσοκομείο.

9.1.2.1.5. Κατά την εγκατάσταση λογισμικού που δεν αναπτύχθηκε από το νοσοκομείο, θα πρέπει να τηρούνται τα εξής:

- Το λογισμικό θα πρέπει να συμμορφώνεται στα καθορισμένα μέτρα ασφάλειας.

- Να ελεγχθεί κατά την παραλαβή του ως προς την ασφάλεια.

9.1.2.2. Ασφάλεια σχετικά με ασθενείς και πολίτες.

Έλεγχοι και διαδικασίες στις συναλλαγές με πολίτες και ασθενείς.

9.1.2.2.1. Το νοσοκομείο θα παρέχει την απαιτούμενη ενημέρωση στους ασθενείς σχετικά με την επεξεργασία των προσωπικών τους δεδομένων.

Η ενημέρωση θα γίνεται με ειδικό έγγραφο που θα δίνεται στους ασθενείς και συμπληρωματικά, με ανάρτηση ενημερωτικών πινακίδων σε εμφανή σημεία και ανάρτηση ενημερωτικού κειμένου στην ιστοσελίδα του νοσοκομείου.

9.1.2.2.2. Στους ασθενείς πρέπει να υπάρχει καθορισμένη διαδικασία για την έκδοση και παράδοση εγγράφων που εμπεριέχουν ευαίσθητα προσωπικά δεδομένα των ασθενών.

Αυτά τα έγγραφα είναι:

Βεβαιώσεις νοσηλείας – Βεβαιώσεις ΤΕΠ

9.2 Διαχείριση Αγαθών

Μέτρα για τη προστασία των πληροφοριακών αγαθών αλλά και των φυσικών αγαθών που περιέχουν εμπιστευτικά ή απόρρητα δεδομένα όπως ο Φάκελος Ασθενή.

9.2.1. Ευθύνη για τα αγαθά

Διαχείριση της ασφάλειας των πληροφοριακών αγαθών του νοσοκομείου.

9.2.1. 1. Καταγραφή πληροφοριακών αγαθών

Πρέπει να υπάρχει λεπτομερής καταγραφή του πληροφοριακού εξοπλισμού του νοσοκομείου.

9.2.1.1.1. Πρέπει να γίνει καταγραφή των πληροφοριακών αγαθών όπου θα περιλαμβάνονται:

- Το αγαθό

- Την περιγραφή του

- Τα δεδομένα που επεξεργάζεται

- Την τοποθεσία που βρίσκεται

9.2.1.1.1. Η καταγραφή πρέπει να αναθεωρείται τουλάχιστον σε ετήσια βάση.

9.2.2. Ιδιοκτησία των αγαθών

9.2.2.1. Κάθε αγαθό πρέπει να έχει ένα ιδιοκτήτη που θα καταγράφεται στον κατάλογο των αγαθών.

9.2.3. Αποδεκτή χρήση των αγαθών

9.2.2.2. Τα πληροφοριακά αγαθά θα πρέπει να χρησιμοποιούνται σύμφωνα με την Ελληνική και διεθνή νομοθεσία και τις απαιτήσεις της ΑΠΔΠΧ.

9.2.4. Ταξινόμηση πληροφοριών

Οι πληροφορίες θα ταξινομούνται και η προστασία που λαμβάνουν θα είναι ανάλογη της ταξινόμησης αυτής

9.2.4.1. Οδηγίες ταξινόμησης πληροφοριών

Η ταξινόμηση γίνεται σε συνάρτηση με την αξία τους, τις νομικές απαιτήσεις, την ευαισθησία και την κρισιμότητά τους.

9.2.4.1.1. Ο Υπεύθυνος Ασφάλειας σε συνεργασία με τους ιδιοκτήτες των πληροφοριακών αγαθών θα ταξινομεί τις πληροφορίες.

Οι κατηγορίες ταξινόμησης των πληροφοριών θα είναι:

- Δημόσιες

- Δεδομένα Προσωπικού Χαρακτήρα

- Δεδομένα που εμπίπτουν στο Ιατρικό Απόρρητο

9.3 Ασφάλεια Ανθρώπινων Πόρων

Να διασφαλιστεί ότι οι εργαζόμενοι, οι εργολάβοι και οι τρίτοι χρήστες κατανοούν τις ευθύνες τους, και να είναι κατάλληλοι για τους ρόλους για τους οποίους εξετάζονται, και να μειώνει τον κίνδυνο της κλοπής, απάτης ή κατάχρησης των εγκαταστάσεων.

9.3.1 Ασφάλεια που προηγείται ανάθεσης εργασίας στο προσωπικό

Απαιτούμενοι έλεγχοι σε υπαλλήλους πριν αναλάβουν εργασίες σχετικά με το ΟΠΣΝ.

9.3.1.1. Ρόλοι και αρμοδιότητες

Οι ρόλοι ασφάλειας και οι ευθύνες των εργαζομένων, αναδόχων και τρίτων χρηστών θα πρέπει να καθορίζονται και να τεκμηριώνονται σύμφωνα με την πολιτική ασφάλειας του νοσοκομείου.

9.3.1.1.2 Οι εργαζόμενοι θα ενημερώνονται σαφώς για την κρισιμότητα της εργασίας που αναλαμβάνουν και τις ευθύνες τους σχετικά με την ασφάλεια.

9.3.1.1.3 Δεν θα πρέπει να υπάρχουν εργασίες διαχείρισης για τις οποίες μόνο ένα μέρος του προσωπικού θα έχει τις απαιτούμενες γνώσεις εκτέλεσης.

9.3.2 Ασφάλεια προσωπικού κατά τη διάρκεια της εργασίας

Πρέπει να διασφαλιστεί ότι οι εργαζόμενοι, ανάδοχοι και τρίτοι χρήστες έχουν επίγνωση για τις ανησυχίες, τις ευθύνες και τις υποχρεώσεις τους και είναι επαρκώς καταρτισμένοι για την ελαχιστοποίηση των κινδύνων ασφάλειας.

9.3.2.1. Ευαισθητοποίηση, ενημέρωση και εκπαίδευση για την ασφάλεια

9.3.2.1.1. Οι εργαζόμενοι θα ενημερώνονται και θα εκπαιδεύονται για την εργασία που αναλαμβάνουν και τα μέτρα που θα λαμβάνουν σχετικά με την ασφάλεια.

9.3.2.1.2. Οι εργαζόμενοι που δεν δεσμεύονται από το ιατρικό απόρρητο, θα λαμβάνουν γνώση του «**Κώδικα Δεοντολογίας**» του νοσοκομείου.

9.3.2.1.3. Οι εργαζόμενοι θα ενημερώνονται για τις διαδικασίες που θα ακολουθήσουν σε περίπτωση περιστατικού παραβίασης της ασφάλειας.

9.3.2.2. Διαδικασία συμμόρφωσης

9.3.2.2.1. Οι εργαζόμενοι θα ενημερώνονται για τις νομικές κυρώσεις σε περίπτωση παραβίασης της ασφάλειας.

9.3.2.2.2. Οι εργαζόμενοι δεσμεύονται από τον «**Κώδικα Δεοντολογίας**» του νοσοκομείου .

9.3.2.2.3. Πρέπει να υπογράφεται σύμβαση εμπιστευτικότητας με τους αναδόχους και τρίτες εταιρείες.

9.3.3. Ασφάλεια κατά την αλλαγή ή τον τερματισμό της εργασίας

Πρέπει να διασφαλιστεί ότι μετά τη λήξη εργασίας οι εργαζόμενοι, ανάδοχοι και τρίτοι χρήστες δεν θα έχουν πρόσβαση στα πληροφοριακά αγαθά της εργασίας τους.

9.3.3.1. Επιστροφή των αγαθών

9.3.3.1.1. Οι εργαζόμενοι που αποχωρούν ή μετατίθενται θα επιστρέφουν ότι εξοπλισμό διαθέτουν στη διοίκηση.

9.3.3.1.2. Θα απενεργοποιούνται άμεσα οι λογαριασμοί πρόσβασης των εργαζόμενων που αποχωρούν ή μετατίθενται.

9.4 Φυσική Ασφάλεια κα Ασφάλεια Περιβάλλοντος

9.4.1. Ασφαλείς περιοχές

Έλεγχοι για την αποτροπή μη εξουσιοδοτημένης φυσικής πρόσβασης στις εγκαταστάσεις του νοσοκομείου, των ΚΥ και των ΠΙ.

9.4.1.1. Φυσική περίμετρος ασφάλειας

Φυσικά μέτρα προστασίας μη εξουσιοδοτημένης πρόσβασης σε χώρους του νοσοκομείου, των ΚΥ και των ΠΙ.

9.4.1.1.1. Θα υπάρχει προσωπικό φύλαξης σε 24ωρη βάση για τον έλεγχο της πρόσβασης στο νοσοκομείο, στα ΚΥ και στα ΠΙ.

9.4.1.1.2. Τα κλειδιά θα φυλάσσονται σε ασφαλές μέρος και θα οριστούν υπεύθυνοι διαχείρισης τους.

9.4.1.1.3. Τα κλειδιά ή οι συνδυασμοί κλειδαριών θα αλλάζουν όποτε μέλη του προσωπικού που τα χρησιμοποιούσαν και αφορούσαν σε κρίσιμες λειτουργίες αποχωρούν ή αλλάζουν.

9.4.1.1.4. Οι επισκέπτες των ασθενών θα εισέρχονται μόνο το προκαθορισμένο ωράριο επίσκεψης.

9.4.1.1.5. Οι επισκέπτες των ασθενών θα προμηθεύονται σήμα επισκέπτη το οποίο θα φέρουν κατά τη διάρκεια της επίσκεψης.

9.4.1.2. Προστασία δωματίου εξυπηρετητών

9.4.1.2.1. Οι εξυπηρετητές θα στεγάζονται σε ειδικό ασφαλισμένο χώρο (Computer room).

9.4.1.2.3. Το δωμάτιο εξυπηρετητών παραμένει πάντα κλειδωμένο.

- Μόνο το προσωπικό το ΤΠΟ και της ΥΠε έχει δικαίωμα πρόσβασης στο δωμάτιο εξυπηρετητών.

- Αν παραστεί ανάγκη πρόσβασης σε τρίτους, αυτό θα γίνεται με συνοδεία υπαλλήλου του ΤΠΟ.

9.4.1.2.4. Στο δωμάτιο εξυπηρετητών θα υπάρχουν τα παρακάτω συστήματα:

- *Σύστημα πυρανίχνευσης και πυρόσβεσης*
- *Σύστημα συναγερμού*
- *Κλιματισμό*

9.4.1.2.5. Το δωμάτιο εξυπηρετητών να υποστηρίζεται από Ηλεκτροπαραγωγά Ζεύγη.

Το σύστημα να επαρκεί για την λειτουργία όλου του εξοπλισμού, εξυπηρετών, κλιματισμού και των συστημάτων πυρανίχνευσης.

9.4.1.2.6. Το δωμάτιο εξυπηρετητών να υποστηρίζεται από συσκευή αδιάλειπτης παροχής ενέργειας (UPS).

Το σύστημα να επαρκεί για την λειτουργία όλου του εξοπλισμού, εξυπηρετών, κλιματισμού και των συστημάτων πυρανίχνευσης, έως ότου αποκατασταθεί η κανονική ηλεκτροδότηση.

9.4.1.2.7. Να μην χρησιμοποιούνται συσκευές επικίνδυνες για πρόκληση πυρκαγιάς στο δωμάτιο εξυπηρετητών.

9.4.1.2.8. Να μην αποθηκεύονται μόνιμα ή προσωρινά υλικά που δεν είναι απαραίτητα για την λειτουργία των ΠΣ (χαρτιά, εκτυπώσεις κλπ).

9.4.1. Ασφάλεια Εξοπλισμού

Έλεγχοι για την αποτροπή απώλειας, καταστροφής, κλοπής ή παραβίασης των αγαθών του νοσοκομείου, των ΚΥ και των ΠΙ.

9.4.1.2. Ασφάλεια στην πρόσβαση σε συσκευές

Φυσικά μέτρα προστασίας μη εξουσιοδοτημένης πρόσβασης σε σταθμούς εργασίας και δικτυακό εξοπλισμό.

9.4.1.2.1. Οι σταθμοί εργασίας θα βρίσκονται σε μέρη που αποτρέπουν την μη ελεγχόμενη φυσική πρόσβαση σε αυτούς.

9.4.1.2.2. Η πρόσβαση στους σταθμούς εργασίας θα ελέγχεται με τη χρήση μοναδικών ατομικών αναγνωριστικού χρήστη και συνθηματικού.

9.4.1.2.3. Οι χρήστες δεν θα έχουν δικαιώματα διαχειριστή και δεν θα εγκαθιστούν εφαρμογές ή συσκευές.

9.4.1.2.4. Οι συσκευές δικτύου θα εγκαθίστανται σε ειδικούς φωριαμούς οι οποίοι θα μένουν κλειδωμένοι.

9.4.1.3. Συντήρηση εξοπλισμού

Ο εξοπλισμός θα πρέπει να συντηρείται τακτικά είτε από ανάδοχο είτε από προσωπικό του ΤΠΟ.

9.4.1.3.1. Να υπάρχει συμβόλαιο συντήρησης για όλα τα σημαντικά στοιχεία του εξοπλισμού.

9.4.1.3.2. Το ΤΠΟ θα παρακολουθεί τα συμβόλαια συντήρησης για όλα τα σημαντικά στοιχεία του εξοπλισμού και θα φροντίζει για την έγκαιρη ανανέωσή τους.

9.4.1.3.3. Το ΤΠΟ θα καταγράφει όλες τις βλάβες του εξοπλισμού και τις διαδικασίες αποκατάστασής τους.

9.4.1.3.4. Επισκευή συσκευών που περιέχουν ευαίσθητα προσωπικά δεδομένα θα γίνεται εντός του νοσοκομείου. Αν πρέπει υποχρεωτικά να επισκευαστούν εκτός θα πρέπει να λαμβάνονται τα απαραίτητα μέτρα προστασίας.

9.4.1.4. Προστασία από φυσικούς και περιβαλλοντικούς κινδύνους

Ο εξοπλισμός θα πρέπει να προστατεύεται από φυσικές καταστροφές ή περιβαλλοντικούς κινδύνου.

9.4.1.4.1. Θα ληφθούν τα παρακάτω μέτρα για την προστασία του εξοπλισμού από πλημμύρα.

- *Να ελέγχονται οι σωληνώσεις (ύδρευσης, θέρμανσης κλπ.) για πιθανές ευπάθειες.*

- *Να μην διέρχονται τέτοιου είδους σωληνώσεις από τα δωμάτια εξυπηρετητών.*

- *Οι βαλβίδες ελέγχου παροχής νερού να είναι εύκολα προσβάσιμες και να έχουν ενδείξεις για τη θέση τους*

9.4.1.4.2. Να υπάρχει αντικεραυνική προστασία στα κτίρια που στεγάζουν κρίσιμα στοιχεία του εξοπλισμού.

9.5 Διαχείριση Επικοινωνιών και Λειτουργιών

Οι αρμοδιότητες και διαδικασίες για τη διαχείριση και λειτουργία όλων των εγκαταστάσεων επεξεργασίας πληροφοριών πρέπει να καθοριστούν. Αυτό περιλαμβάνει την ανάπτυξη των κατάλληλων διαδικασιών λειτουργίας.

9.5.1. Λειτουργικές διαδικασίες και αρμοδιότητες

Έλεγχοι για την σωστή και ασφαλή λειτουργία των εγκαταστάσεων επεξεργασίας των πληροφοριών.

9.5.1.1. Τεκμηρίωση των λειτουργικών διαδικασιών

Οι διαδικασίες λειτουργίας πρέπει να τεκμηριώνονται, καταγράφονται και να διατίθενται σε όλους τους χρήστες.

9.5.1.1.1. Ο Υπεύθυνος Ασφάλειας θα είναι επιφορτισμένος με την επικοινωνία με τους χρήστες σε περίπτωση που χρειαστούν βοήθεια για την αντιμετώπιση λαθών ή έκτακτων συνθηκών που ενδέχεται να προκύψουν κατά την εκτέλεση της εργασίας.

9.5.1.1.2. Το προσωπικό του ΤΠΟ θα είναι επιφορτισμένο με την επικοινωνία με τους χρήστες σε περίπτωση που χρειαστούν βοήθεια στις επιχειρησιακές διαδικασίες του ΠΣ.

9.5.1.1.3. Θα συνταχθεί έγγραφο τεκμηρίωσης όπου οι διαδικασίες για τη χρήση υποσυστημάτων του ΟΠΣΝ θα είναι καταγεγραμμένες και διαθέσιμες στους χρήστες αυτών.

9.5.1.1.4. Θα τηρείται «**Μητρώο Μεταβολών Λογισμικού**» το οποίο περιλαμβάνει:

- *Μοναδικό σειριακό αριθμό της μεταβολής*
- *Περιγραφή της μεταβολής*
- *Ημερομηνία μεταβολής*
- *Αιτία μεταβολής*
- *Όνομα αιτούντος τη μεταβολή*

9.5.1.1.5. Θα τηρείται «**Μητρώο Πληροφοριακού Εξοπλισμού**» το οποίο περιλαμβάνει:

- *Μοναδικό σειριακό αριθμό Υλικού*
- *Περιγραφή Υλικού*
- *Τμήμα Εγκατάστασης*
- *Λογισμικό που μπορεί να έχει*
- *Ιδιοκτήτη*

9.5.1.1.6. Θα συνταχθεί έγγραφο αντιμετώπιση επιβλαβούς λογισμικού με τις απαραίτητες οδηγίες προς το προσωπικό του νοσοκομείου.

Οι οδηγίες θα είναι σχετικές με τα εξής:

- *Διαχείριση ηλεκτρονικού ταχυδρομείου*
- *Διαχείριση μηνυμάτων ηλεκτρονικού ταχυδρομείου με επισυναπτόμενα εκτελέσιμα αρχεία*
- *Διαχείριση αρχείων από το Διαδίκτυο*

9.5.1.1.6. Θα συνταχθεί έγγραφο με οδηγίες λήψης εφεδρικών δεδομένων και επαναφοράς τους.

9.5.1.1.7. Θα συνταχθεί έγγραφο καταγραφής περιστατικών ασφάλειας.

Το έγγραφο θα περιλαμβάνει:

- *Ημερομηνία συμβάντος*
- *Περιγραφή συμβάντος*
- *Διαδικασία αντιμετώπισης*

9.5.1.1.7. Θα τηρείται «**Μητρώο Προβλημάτων Δικτύου**».

Το Μητρώο Προβλημάτων Δικτύου θα περιλαμβάνει:

- *Ημερομηνία συμβάντος*
- *Περιγραφή συμβάντος*
- *Διαδικασία αντιμετώπισης*

9.5.1.2. Διαχείριση των μεταβολών

Έλεγχοι των μεταβολών στις εγκαταστάσεις επεξεργασίας των πληροφοριών και των συστημάτων.

9.5.1.2.1. Τροποποίηση του λογισμικού προϋποθέτει την έγκριση των αντίστοιχων υπευθύνων.

9.5.1.2.2. Τροποποίηση του λογισμικού πρέπει να εξετάζεται αν επηρεάζει την ασφάλεια του ΠΣ και να εγκρίνεται από τον Υπεύθυνο Ασφάλειας του ΠΣ.

9.5.1.2.3. Οι τροποποιήσεις του λογισμικού θα πραγματοποιούνται πρώτα σε δοκιμαστικό περιβάλλον και μετά σε παραγωγική λειτουργία.

9.5.1.2.4. Θα ενημερώνεται το μητρώο μεταβολών.

9.5.1.2.5. Η μεταβολή θα καταγράφεται στο έγγραφο τεκμηρίωσης.

9.5.1.3. Καθορισμός καθηκόντων

Τα καθήκοντα και οι τομείς ευθύνης θα πρέπει να καθορίζονται, προκειμένου να μειωθούν οι ευκαιρίες για την μη εξουσιοδοτημένη ή ακούσια τροποποίηση ή κακή χρήση των πληροφοριακών αγαθών του νοσοκομείου.

9.5.1.3.1. Να γίνονται οι απαραίτητες αναβαθμίσεις (updates, patches κλπ) που εκδίδονται από τον κατασκευαστή του λειτουργικού.

9.5.1.3.2. Να αλλάζουν ή να αναβαθμίζονται τα λειτουργικά συστήματα που δεν υποστηρίζονται πλέον από τον κατασκευαστή τους.

9.5.1.3.3. Οι αλλαγές των λειτουργικών να γίνονται σε συνεργασία με τον Υπεύθυνο Ασφάλειας του ΠΣ.

9.5.1.3.4. Να ενημερώνεται το μητρώο αγαθών για τις αλλαγές των λειτουργικών.

9.5.2. Διαχωρισμός παραγωγικού περιβάλλοντος από το περιβάλλον ανάπτυξης και το δοκιμαστικό περιβάλλον

Η ανάπτυξη, η δοκιμή και παραγωγική λειτουργία θα πρέπει να διαχωρίζονται για να μειωθούν οι κίνδυνοι από μη εξουσιοδοτημένη πρόσβαση ή αλλαγές στο λειτουργικό σύστημα.

9.5.2.1. Διαχείριση ασφάλειας σε παροχή υπηρεσιών από τρίτους

Έλεγχοι για την ασφάλεια των πληροφοριών και την παροχή υπηρεσιών από τρίτους.

9.5.2.1.1. Οι εξωτερικοί συνεργάτες θα διατηρούν το απαραίτητο επίπεδο παροχής υπηρεσιών σε συνδυασμό με τις απαιτήσεις ασφάλειας του νοσοκομείου.

9.5.2.1.2. Παρακολούθηση και έλεγχος των υπηρεσιών τρίτων για να διασφαλιστεί ότι οι όροι της ασφάλειας των πληροφοριών και των όρων των συμφωνιών τηρούνται και ότι τα περιστατικά ασφάλειας των πληροφοριών και τα προβλήματα διαχειρίζονται σωστά.

9.5.2.2. Διαχείριση ων μεταβολών στις υπηρεσίες τρίτων

Έλεγχοι των μεταβολών στις υπηρεσίες τρίτων, λαμβάνοντας υπόψη την κρισιμότητα των συστημάτων και των διαδικασιών και την εκ νέου εκτίμηση των κινδύνων.

9.5.2.2.1. Τροποποίηση του λογισμικού προϋποθέτει την έγκριση των αντίστοιχων υπευθύνων.

9.5.3. Σχεδιασμός συστήματος και αποδοχή

Έλεγχοι για να ελαχιστοποιηθεί ο κίνδυνος αστοχιών του συστήματος.

9.5.3.1. Διαχείριση χωρητικότητας

Έλεγχοι διασφάλισης των απαιτήσεων χωρητικότητας.

9.5.3.1.1. Τα αποθηκευτικά μέσα θα ελέγχονται ώστε να έχουν την απαιτούμενη χωρητικότητα.

9.5.3.1.2. Τα αποθηκευτικά μέσα θα συντηρούνται σύμφωνα με τις απαιτήσεις του κατασκευαστή.

9.5.3.2. Αποδοχή του συστήματος

Κριτήρια αποδοχής για τα νέα πληροφοριακά συστήματα, αναβαθμίσεις και νέες εκδόσεις θα πρέπει να καθοριστούν.

9.5.3.2.1. Το νέο ΠΣ θα συμμορφώνεται με τις απαιτούμενες προδιαγραφές εργασίας.

9.5.3.2.2. Το νέο ΠΣ θα συμμορφώνεται με την Πολιτική Ασφάλειας.

9.5.3.2.3. Τροποποιήσεις στο ΟΠΣΝ θα συμμορφώνονται με τις απαιτούμενες προδιαγραφές εργασίας.

9.5.3.2.4. Τροποποιήσεις στο ΟΠΣΝ θα συμμορφώνονται με την Πολιτική Ασφάλειας.

9.5.4. Προστασία από κακόβουλο και κινητό κώδικα

Έλεγχοι για την πρόληψη και τον εντοπισμό της εισαγωγής κακόβουλου κώδικα και μη εξουσιοδοτημένου κινητού κώδικα.

9.5.4.2. Έλεγχοι για κακόβουλο κώδικα

Έλεγχοι ανίχνευσης, πρόληψης και διαδικασία αποκατάστασης για την προστασία από κακόβουλο κώδικα και κατάλληλες διαδικασίες ευαισθητοποίησης των χρηστών που πρέπει να εφαρμοστούν

9.5.4.2.1. Να εγκατασταθεί λογισμικό ανίχνευση ιομορφικού λογισμικού σε όλους τους σταθμούς εργασίας και στους εξυπηρετητές. Το λογισμικό πρέπει:

- *Να προέρχεται από αξιόπιστους κατασκευαστές*
- *Να ενημερώνεται τουλάχιστον μια φορά την εβδομάδα*

9.5.4.2.2. Να δοθεί το έγγραφο αντιμετώπισης επιβλαβούς λογισμικού στο προσωπικό του νοσοκομείου.

9.5.4.2.3. Σε περίπτωση ανίχνευσης ιομορφικού λογισμικού θα γίνονται οι παρακάτω ενέργειες:

- *Διακοπή τρέχουσας δραστηριότητας*
- *Απομόνωση του συγκεκριμένου Η/Υ*
- *Πληροφόρηση του αρμόδιου προσωπικού*
- *Λήψη αντιγράφου του ιομορφικού λογισμικού*
- *Ακριβής προσδιορισμός του προβλήματος σχετικά με το ιομορφικό λογισμικό*
- *Διαγραφή του ιομορφικού λογισμικού*
- *Ανάκτηση του συστήματος*

9.5.4.2.4. Να ενημερώνεται το προσωπικό για θέματα ασφάλειας από επιβλαβή κώδικα

9.5.4.3. Έλεγχοι για κινητό κώδικα

Σε περίπτωση που η χρήση κινητού κώδικα επιτρέπεται, η διαμόρφωση πρέπει να εξασφαλίζει ότι ο εγκεκριμένος κινητός κώδικας λειτουργεί σύμφωνα με την πολιτική ασφαλείας του νοσοκομείου.

9.5.4.3.1. Θα υπάρξει απαραίτητη τεκμηρίωση για την αναγκαιότητα χρήσης κινητού κώδικα.

9.5.4.3.2. Ο Υπεύθυνος Ασφαλείας θα ελέγξει να η χρήση του κινητού κώδικα επηρεάζει την πολιτική ασφάλειας του νοσοκομείου.

9.5.4.3.3. Θα επιτρέπεται μόνο ο αναγκαίος κινητός κώδικας.

9.5.5. Αντίγραφα Ασφάλειας

Διαδικασίες λήψης αντιγράφων ασφάλειας δεδομένων και λογισμικού.

9.5.5.1. Αντίγραφα ασφάλειας πληροφοριών

Έλεγχοι για την λήψη αντιγράφων ασφαλείας και εξασφάλιση επαναφοράς του ΠΣ μετά από μια καταστροφή ή βλάβη.

9.5.5.1.1. Θα λαμβάνονται αντίγραφα δεδομένων με τρεις ανεξάρτητες διεργασίες:

- *Ημερήσια*
- *Εβδομαδιαία*
- *Μηνιαία*

9.5.5.1.2. Θα λαμβάνονται αντίγραφα και του λογισμικού των συστημάτων (full system back up).

9.5.5.1.3. Τα εφεδρικά αντίγραφα δεδομένων θα φυλάσσονται ως εξής:

- *Θα βρίσκονται σε ξεχωριστό χώρο από τα πρωτότυπα*
- *Οι χώροι αυτοί θα ελέγχονται για την πρόσβαση από μη εξουσιοδοτημένο προσωπικό*
- *Οι χώροι αυτοί θα προστατεύονται από φυσικές και περιβαλλοντικές καταστροφές*

9.5.5.1.4. Θα τηρούνται τουλάχιστον τρεις γενιές εφεδρικών αντιγράφων ασφάλειας

9.5.5.1.5. Τα εφεδρικά αντίγραφα να είναι πλήρη και όχι αυξητικά.

9.5.5.1.6. Κάθε εφεδρικό αντίγραφο να φέρει κωδικό αναγνώρισης.

Ο κωδικός αναγνώρισης θα χρησιμοποιείται για την αντιστοίχηση του αντιγράφου με τα δεδομένα που περιέχει και τις αντίστοιχες εφαρμογές και θα αναγράφεται και η διαβάθμιση των δεδομένων

9.5.5.1.7. Να γίνεται έλεγχος αποκατάστασης από τα εφεδρικά δεδομένα μια φορά το χρόνο.

9.5.5.1.8. Τα αποθηκευτικά μέσα να συντηρούνται σύμφωνα με τις προδιαγραφές των κατασκευαστών τους.

9.5.5.1.9. Για κάθε νέο σύστημα να υπάρχει μέριμνα για τις αναγκαίες διαδικασίες λήψης αντιγράφων.

9.5.6. Διαχείριση Ασφάλειας Δικτύου

Έλεγχοι για την ασφάλεια των πληροφοριών στις δικτυακές υποδομές.

9.5.6.1. Έλεγχοι δικτύου

Οι διαχειριστές δικτύων θα πρέπει να εφαρμόσουν τους ελέγχους για τη διασφάλιση της ασφάλειας των πληροφοριών σε δίκτυα και την προστασία των συνδεδεμένων υπηρεσιών από μη εξουσιοδοτημένη πρόσβαση.

9.5.6.1.1. Για κάθε νέο σύστημα να υπάρχει μέριμνα για τις αναγκαίες Το εσωτερικό υποδίκτυο του νοσοκομείου θα είναι ανεξάρτητο δίκτυο από το δίκτυο του ΟΠΣΥ της ΥΠε.

9.5.6.1.2. Τα υποδίκτυα θα επικοινωνούν μεταξύ τους και η επικοινωνία θα ρυθμίζεται μέσω αναχώματος ασφάλειας με κανόνες φιλτραρίσματος πακέτων που θα επιτρέπουν μόνο την απολύτως αναγκαία επικοινωνία.

9.5.6.1.3. Οι κεντρικοί εξυπηρετητές θα προστατεύονται από ανάχωμα ασφάλειας.

9.5.6.1.4. Τα αναχώματα ασφάλειας και οι δρομολογητές θα ρυθμιστούν έτσι ώστε να μην είναι εφικτό να τα διαχειριστεί κάποιος από το εξωτερικό δίκτυο.

9.5.6.1.5. Οι IP διευθύνσεις των εσωτερικών κόμβων το δικτύου να μην είναι προσβάσιμες ή ανιχνεύσιμες από εξωτερικά δίκτυα όπως το Διαδίκτυο ή το Σύζευξις.

9.5.6.1.6. Να ελέγχεται η εισερχόμενη και εξερχόμενη κίνηση για κακόβουλο λογισμικό.

9.5.6.1.7. Να εφαρμοστεί NAT (Network Address Translation).

9.5.6.1.8. Να ρυθμιστούν οι ενεργές θύρες (ports) ώστε να είναι inbound, outbound ή bidirectional, ανάλογα με τις υπηρεσίες που υποστηρίζουν.

9.5.6.1.9. Να οριστεί πολιτική ελέγχου πρόσβασης αναχωμάτων ασφάλειας.

9.5.6.1.10. Να ελέγχεται ανά εξάμηνο αν εφαρμόζεται σωστά η πολιτική ελέγχου των αναχωμάτων.

9.5.6.1.11. Να γίνεται περιοδικά έλεγχος ανθεκτικότητας (penetration testing).

9.5.6.2. Ασφάλεια υπηρεσιών δικτύου

Οι ρυθμίσεις ασφαλείας που απαιτούνται για συγκεκριμένες υπηρεσίες, όπως χαρακτηριστικά ασφαλείας, τα επίπεδα εξυπηρέτησης και οι απαιτήσεις διαχείρισης.

9.5.6.2.1. Τα περιστατικά ασφάλειας θα αναφέρονται στον Υπεύθυνο Ασφάλειας.

9.5.6.2.2. Θα ενημερώνεται το Μητρώο Προβλημάτων Δικτύου όταν παρουσιάζεται ένα πρόβλημα.

9.5.6.2.3. Οι συσκευές δικτύου θα τοποθετούνται σε χώρο που δεν έχει πρόσβαση το κοινό.

9.5.6.2.4. Απαγορεύονται οι παρεμβάσεις στη δικτύωση χωρίς έγκριση του Υπεύθυνου Ασφάλειας και του ΤΠΟ.

9.5.6.2.5. Να παρακολουθείται το δίκτυο ώστε να ανιχνεύονται έγκαιρα αστοχίες του υλικού, του λογισμικού, μη εξουσιοδοτημένη χρήση κλπ.

Για την εποπτεία του δικτύου θα χρησιμοποιηθεί κατάλληλο λογισμικό διαχείρισης δικτύων.

9.5.6.2.6. Οι διαθέσιμες υπηρεσίες του Διαδικτύου να περιορισθούν στις απαραίτητες.

9.5.7. Χειρισμός Μέσων

Έλεγχοι για την ασφάλεια εγγράφων, μέσων πληροφορικής (π.χ. ταινίες, δίσκους), δεδομένα εισόδου / εξόδου και την τεκμηρίωση του συστήματος.

9.5.7.1. Διαχείριση αφαιρούμενων μέσων

Διαδικασίες για τη διαχείριση των αφαιρούμενων μέσων

9.5.7.1.1. Στους σταθμούς εργασίας όπου γίνεται επεξεργασία εμπιστευτικών δεδομένων δεν θα υπάρχουν ή θα είναι απενεργοποιημένα τα:

- *Οδηγοί οπτικών δίσκων*
- *Οδηγοί δισκέτας*
- *Θύρες USB*

9.5.7.2. Απόρριψη αφαιρούμενων μέσων

Καθορισμός διαδικασιών ασφάλειας των πληροφοριών κατά την απόρριψη μέσων.

9.5.7.2.1. Αφαιρούμενα μέσα που απορρίπτονται πρέπει πρώτα να καταστρέφονται και να καθίσταται αδύνατη η ανάγνωση δεδομένων από αυτά.

9.5.7.2.2. Έγγραφα και έντυπο υλικό που απορρίπτονται πρέπει πρώτα να καταστρέφονται και να καθίσταται αδύνατη η ανάγνωση δεδομένων από αυτά.

9.5.7.2.3. Για την απόρριψη των αφαιρούμενων μέσων και εγγράφων θα ακολουθείται η οδηγία της ΑΠΔΠΧ.

9.5.7.4. Ασφάλεια της τεκμηρίωσης του συστήματος

Έλεγχοι για την προστασία της τεκμηρίωσης του συστήματος η οποία μπορεί να περιλαμβάνει ευαίσθητες πληροφορίες.

9.5.7.4.1. Δεδομένα σε ηλεκτρονική ή σε έγγραφη μορφή που αφορούν στην τεκμηρίωση του συστήματος θα προστατεύονται ακολουθώντας τα μέτρα που έχουν οριστεί για τα εμπιστευτικά δεδομένα.

9.5.8. Ανταλλαγή πληροφοριών

Έλεγχοι για την ασφάλεια των πληροφοριών και του λογισμικού που ανταλλάσσονται εσωτερικά στο νοσοκομείο ή με οποιαδήποτε εξωτερική οντότητα.

9.5.8.1. Πολιτική και διαδικασίες ανταλλαγής πληροφοριών

Οι διαδικασίες και οι έλεγχοι που πρέπει να ακολουθούνται κατά τη χρήση ηλεκτρονικής επικοινωνίας για την ανταλλαγή πληροφοριών.

9.5.8.1.1. Οι πληροφορίες που ανταλλάσσονται εκτός του νοσοκομείου θα προστατεύονται με κρυπτογραφικές μεθόδους.

9.5.8.1.2. Να χρησιμοποιούνται κρυπτοσυστήματα αξιόπιστων κατασκευαστών.

9.5.8.1.3. Ο Υπεύθυνος Ασφάλειας να ενημερώνεται για τις εξελίξεις στο χώρο της κρυπτογραφίας και κρυπτανάλυσης ώστε να επιλέγονται οι πλέον αξιόπιστες για το νοσοκομείο.

9.5.8.2. Συμβάσεις ανταλλαγής

Οι συμβάσεις που πρέπει να θεσπιστούν για την ανταλλαγή πληροφοριών και λογισμικού μεταξύ του οργανισμού και των εξωτερικών μερών.

9.5.8.2.1. Ο Υπεύθυνος Εξωτερικοί συνεργάτες ή τρίτα μέρη που έχουν πρόσβαση στο ΟΠΣΝ θα πρέπει να δεσμεύονται ρητά μέσω υπογραφής συμβάσεων για την τήρηση της Πολιτικής Ασφάλειας του νοσοκομείου.

9.5.8.3. Ηλεκτρονικά μηνύματα

Διαδικασίες προστασίας των πληροφοριών που αποστέλλονται με ηλεκτρονικά μηνύματα.

9.5.8.3.1. Εμπιστευτικές πληροφορίες και προσωπικά δεδομένα θα διακινούνται κρυπτογραφημένα μέσω ηλεκτρονικού ταχυδρομείου.

9.5.8.4. Επιχειρησιακό ΠΣ

Διαδικασίες που πρέπει να ακολουθούνται για την προστασία των πληροφοριών που σχετίζονται με τη διασύνδεση των πληροφοριακών συστημάτων του νοσοκομείου.

9.5.8.4.1. Η συλλογή πληροφοριών από τα επιμέρους συστήματα του ΠΣ δεν θα περιέχει ευαίσθητα προσωπικά δεδομένα.

9.5.8.5. Υπηρεσίες εξυπηρέτησης πολιτών

Προστασία των πληροφοριών που διατίθενται μέσω ενός κοινού συστήματος θα πρέπει να προστατεύονται ώστε να αποτρέπεται η μη εξουσιοδοτημένη τροποποίηση.

9.5.8.5.1. Οι ενημερωτικές πληροφορίες που αναρτούνται στον ιστοχώρο του νοσοκομείου θα ελέγχονται τακτικά από τον Υπεύθυνο Συντήρησης του Ιστοχώρου.

9.5.9. Παρακολούθηση

Έλεγχος αρχείων καταγραφής ενεργειών στο ΠΣ.

9.5.9.1. Έλεγχος Σύνδεσης

Έλεγχοι σύνδεσης των χρηστών.

9.5.9.1.1. Θα τηρούνται αρχεία καταγραφής που θα περιλαμβάνουν:

- Ταυτότητα των χρηστών
- Ταυτότητα του σταθμού εργασίας
- Ενέργειες σύνδεσης και αποσύνδεσης
- Επιτυχείς και ανεπιτυχείς προσπάθειες σύνδεσης του χρήστη
- Εκκίνηση και παύση του συστήματος

- Αλλαγές δικαιωμάτων
- Η χρήση των λογαριασμών σε ασυνήθιστες ώρες

9.5.9.1.2. Τα αρχεία καταγραφής θα ελέγχονται τακτικά, ακόμα και αν δεν υπάρξει πρόβλημα ή παραβίαση.

9.5.9.2. Προστασία αρχείων καταγραφής

9.5.9.2.1. Τα αρχεία καταγραφής θα προστατεύονται από πρόσβαση μη εξουσιοδοτημένων ατόμων

9.5.9.2.2. Η διαδικασία για την μεταβολή η διαγραφή τους θα ελέγχεται από τον Υπεύθυνο Ασφάλειας

9.5.9.2.3. Αντίγραφο των αρχείων θα τηρείται σε εφεδρικά μέσα.

9.5.9.2.4. Το σύστημα καταγραφής θα λειτουργεί διαρκώς.

9.5.9.3. Συγχρονισμός ρολογιών

Τα ρολόγια των υποσυστημάτων του ΠΣ θα είναι συγχρονισμένα.

9.5.9.3.1. Ο συγχρονισμός ρολογιών του ΠΣ είναι κρίσιμος γιατί εκτός των άλλων αφορά την καταγραφή της ώρας εισόδου ασθενών στο νοσοκομείο, της ώρας διενέργειας εξετάσεων κλπ, στοιχεία σημαντικά σε περιπτώσεις εισαγγελικών παραγγελιών.

9.5.9.3.2. Ο συγχρονισμός των ρολογιών θα ελέγχεται κάθε εβδομάδα.

9.5.9.3.3. Ο συγχρονισμός των ρολογιών θα ελέγχεται μετά από αλλαγή της ώρας.

9.5.9.3.4. Ο συγχρονισμός των ρολογιών θα ελέγχεται μετά από κάθε τροποποίηση του ΠΣ.

9.6 Έλεγχος Πρόσβασης

Διαδικασίες ελέγχου πρόσβασης στο ΠΣ.

9.6.1. Επιχειρησιακές απαιτήσεις ελέγχου πρόσβασης

Η πρόσβαση στις πληροφορίες, διαδικασίες και τις εγκαταστάσεις επεξεργασίας πληροφοριών θα πρέπει να ελέγχεται βάση τις επιχειρησιακές απαιτήσεις και τις απαιτήσεις ασφαλείας

9.6.1.1. Πολιτική ελέγχου πρόσβασης

Καθορισμός των διαδικασιών, κανόνων και δικαιωμάτων των χρηστών για τον έλεγχο της πρόσβασης στις πληροφορίες.

9.6.1.1.1. Η πολιτική ελέγχου πρόσβασης θα ακολουθεί το ρολο – κεντρικό μοντέλο πρόσβασης (role-based access control).

9.6.1.1.2. Η πολιτική ελέγχου πρόσβασης για κάθε χρήστη ή ομάδα χρήστη θα είναι σαφώς καθορισμένη.

9.6.1.1.3. Ο «Διαχειριστής Ρόλων» δημιουργεί ένα σύνολο ρόλων.

9.6.1.1.4. Σε κάθε ρόλο αντιστοιχεί ένα σύνολο δικαιωμάτων.

9.6.1.1.5. Σε κάθε χρήστη αντιστοιχεί ένα σύνολο ρόλων.

9.6.1.1.6. Κάθε χρήστης μπορεί να αποκτήσει κάποιο δικαίωμα μόνο με ανάθεση ρόλου η οποία συνοδεύεται και από τα αντικείμενα στα οποία μπορεί να ασκήσει τα δικαιώματα που αποκτά ο χρήστης.

9.6.1.1.7. Οι χρήστες επιτρέπεται να χρησιμοποιούν μόνο τις εφαρμογές και τους πόρους που είναι απαραίτητοι για τους ρόλους τους.

9.6.1.1.8. Οι ρόλοι που κατανέμονται στους χρήστες θα είναι οι απολύτως απαραίτητοι για την εκτέλεση των εργασιών που πρέπει να κάνει ο χρήστης.

9.6.1.1.9. Να είναι δυνατή η ανάθεση ρόλου για περιορισμένο χρονικό διάστημα.

9.6.1.1.10. Η αυθεντικοποίηση όλων των χρηστών θα γίνεται με χρήση συνθηματικών.

9.6.1.1.11. Αν η αυθεντικοποίηση του χρήστη ήταν επιτυχής, τότε ο χρήστης αποκτά τα δικαιώματα των ρόλων που του έχουν ανατεθεί.

9.6.2. Διαχείριση πρόσβασης χρηστών

Διαδικασίες για να εξασφαλιστεί η άδεια πρόσβασης των χρηστών και να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση σε συστήματα πληροφοριών.

9.6.2.1. Εγγραφή χρήστη

Καθορισμός των διαδικασιών ελέγχου πρόσβασης για εγγραφή και διαγραφή του χρήστη από το μητρώο.

9.6.2.1.1. Ο νέοι χρήστες των συστημάτων θα υποβάλλουν αίτηση για την απόκτηση λογαριασμού συστήματος/εφαρμογής στο ΤΠΟ.

9.6.2.1.2. Η αίτηση θα πρέπει να έχει εγκριθεί από τον προϊστάμενο του χρήστη και τη Διοίκηση του νοσοκομείου.

9.6.2.1.3. Μετά την έγκριση της αίτησης το ΤΠΟ θα χορηγεί το λογαριασμό στον αιτούντα.

Θα δοθούν στο χρήστη:

Α. Για την πρόσβαση στους σταθμούς εργασίας

- *Αναγνωριστικό χρήστη (User name)*
- *Συνθηματικό χρήστη (password)*

Β. Για την πρόσβαση στις εφαρμογές και υπηρεσίες

- *Αναγνωριστικό χρήστη (User name)*
- *Συνθηματικό χρήστη (password)*

Γ. Οδηγίες για την ασφαλή χρήση των συστημάτων

9.6.2.2. Διαχείριση δικαιωμάτων

Η διαδικασία κατανομής και χρήσης των δικαιωμάτων των χρηστών.

9.6.2.2.1. Κάθε χρήστης θα έχει μόνο τα απαραίτητη δικαιώματα για την διεκπεραίωση της εργασίας του.

9.6.2.2.2. Τα δικαιώματα πρόσβασης και χρήσης θα ελέγχονται κάθε έξι μήνες από τον Υπεύθυνο Ασφάλειας.

9.6.2.2.3. Διαχείριση συνθηματικών των χρηστών

9.6.2.3. Διαδικασίες ανάθεσης συνθηματικών στους χρήστες

9.6.2.3.1. Οι χρήστες θα χρησιμοποιούν ένα ασφαλές προσωρινό συνθηματικό, που θα δίνεται από το ΤΠΟ και το οποίο είναι υποχρεωμένοι να το αλλάξουν στην πρώτη σύνδεσή τους.

9.6.2.3.2. Οι χρήστες θα αλλάζουν τα συνθηματικά κάθε δύο (2) μήνες.

9.6.2.3.3. Οι διαχειριστές θα αλλάζουν τα συνθηματικά κάθε ένα (1) μήνα.

9.6.2.3.4. Οι χρήστες θα ενημερώνονται με αυτοματοποιημένες διαδικασίες τουλάχιστον πέντε (5) μέρες πριν τη λήξη της ισχύς του συνθηματικού ότι πρέπει να το αλλάξουν.

9.6.2.3.5. Τα προνομιακά δικαιώματα των διαχειριστών δεν θα επιτρέπουν μη εξουσιοδοτημένες ενέργειες.

9.6.2.3.6. Η δομή των συνθηματικών θα έχει ως εξής:

- *Το μήκος τους θα είναι τουλάχιστον 8 χαρακτήρες*
- *Θα περιέχουν τουλάχιστον ένα (1) αλφαβητικό χαρακτήρα*
- *Θα περιέχουν τουλάχιστον ένα (1) αριθμητικό χαρακτήρα*

9.6.2.3.7. Θα αποφεύγονται συνθηματικά τα οποία είναι λέξεις που βρίσκονται σε λεξικό.

9.6.2.3.8. Το σύστημα θα εμποδίζει τους χρήστες να επαναχρησιμοποιούν συνθηματικά.

9.6.2.3.9. Το σύστημα θα εμποδίζει τους χρήστες να χρησιμοποιούν συνθηματικά που δεν ακολουθούν την καθορισμένη δομή.

9.6.2.3.10. Τα προσωρινά συνθηματικά θα τηρούν την προκαθορισμένη δομή των συνθηματικών.

9.6.2.3.11. Προσωρινά συνθηματικά που έχουν δοθεί από προμηθευτές θα αλλάζουν αμέσως μετά την εγκατάσταση.

9.6.2.3.12. Τα συνθηματικά θα παραδίδονται στους χρήστες με ασφαλή διαδικασία.

9.6.2.3.13. Τα συνθηματικά δεν θα παραδίδονται στους χρήστες μέσω ηλεκτρονικού ταχυδρομείου.

9.6.2.3.14. Τα συνθηματικά δεν ελέγχονται τακτικά από τον Υπεύθυνο Ασφαλείας για την τήρηση των κανόνων.

9.6.2.4. Επανεξέταση των δικαιωμάτων πρόσβασης των χρηστών

Η διαδικασία επανεξέτασης των δικαιωμάτων πρόσβασης των χρηστών.

9.6.2.4.1. Τα συνθηματικά Ο Υπεύθυνος Ασφάλειας θα ελέγχει μια φορά κάθε έξι μήνες ότι δεν δίνονται περισσότερα δικαιώματα σε χρήστες από όσα είναι απαραίτητα.

9.6.2.4.2. Αν ένας χρήστης αλλάζει αρμοδιότητες και απαιτεί νέα δικαιώματα τα παλιά πρέπει να αφαιρούνται άμεσα.

9.6.3. Καθήκοντα χρηστών

Οι χρήστες θα πρέπει να έχουν επίγνωση των ευθυνών τους για τη διατήρηση αποτελεσματικών ελέγχων πρόσβασης, ιδίως όσον αφορά τη χρήση των κωδικών πρόσβασης και την ασφάλεια του εξοπλισμού χρήστη

9.6.3.1. Χρήση συνθηματικών

Διαδικασίες που πρέπει να ακολουθούν οι χρήστες στη χρήση των συνθηματικών.

9.6.3.1.1. Αν ένας Οι χρήστες θα ενημερώνονται ότι το συνθηματικό πρέπει να είναι μυστικό και δεν επιτρέπεται η αποκάλυψή τους σε τρίτους.

9.6.3.1.2. Σε περίπτωση που ο χρήστης έχει την υποψία ότι το συνθηματικό του έγινε γνωστό σε τρίτους θα ενημερώσει το ΤΠΟ ή τον Υπεύθυνος Ασφάλειας για να αλλαχτεί.

9.6.3.1.3. Οι χρήστες θα ενημερώνονται για τους κανόνες της δομής του συνθηματικού.

9.6.3.1.4. Οι χρήστες δεν πρέπει να καταγραφούν τα συνθηματικά σε εμφανή σημεία για να τα θυμούνται.

9.6.3.2. Πολιτική 'καθαρού' γραφείου και 'καθαρής' οθόνης

Διαδικασία προστασίας των πληροφοριών σε φυσική ή ψηφιακή μορφή κατά την απουσία του χρήστη από τη θέση εργασίας του.

9.6.3.2.1. Οι σταθμοί εργασίας θα κλειδώνουν μετά από κάποιο χρόνο αδράνειας.

- *Ο χρόνος αδράνειας θα είναι μικρότερος των 30 λεπτών*
- *Ο χρήστης θα πρέπει να εισάγει το συνθηματικό του για να χρησιμοποιήσει τον κλειδωμένο σταθμό.*

9.6.3.2.1. Οι χρήστες δεν πρέπει να αφήνουν έγγραφα που περιέχουν ευαίσθητες πληροφορίες αφύλακτα και σε κοινή θέα.

9.6.4. Έλεγχος πρόσβασης στο δίκτυο

Διαδικασίες προστασίας του δικτύου και των δικτυακών υπηρεσιών.

9.6.4.1. Πολιτική χρήσης των υπηρεσιών του δικτύου

Έλεγχοι για την εξουσιοδοτημένη πρόσβαση των χρηστών στις δικτυακές υπηρεσίες.

9.6.3.4.1. Μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στο δίκτυο.

9.6.3.4.2. Η πρόσβαση στο δίκτυο του νοσοκομείου δίνεται από το ΤΠΟ μετά από έγγραφη απαίτηση που έχει εγκριθεί από τη διοίκηση.

9.6.3.4.3. Απαγορεύεται η χρήση του δικτύου του νοσοκομείου για τη διακίνηση παράνομου υλικού (πορνογραφικού, καταπάτησης πνευματικών δικαιωμάτων, ρατσιστικού κλπ).

9.6.3.4.4. Οι διαθέσιμες υπηρεσίες στο διαδίκτυο θα περιοριστούν στις απαραίτητες.

9.6.3.4.5. Τα προβλήματα ασφάλειας του δικτύου θα αναφέρονται στον Υπεύθυνο Ασφάλειας ή στο ΤΠΟ.

9.6.3.4.6. Θα υπάρχει εποπτεία του δικτύου για να ανιχνεύονται άμεσα προβλήματα ασφάλειας ή λειτουργίας του δικτύου.

9.6.3.4.7. Να ελέγχεται η εισερχόμενη και εξερχόμενη κίνηση για κακόβουλο λογισμικό.

9.6.3.4.8. Να υπάρχει εναλλακτική πρόσβαση στο διαδίκτυο σε περίπτωση που το δίκτυο του νοσοκομείου είναι εκτός λειτουργίας.

9.6.4.2. Προστασία κατά την απομακρυσμένη σύνδεση χρηστών.

9.6.4.2.1. Ευαίσθητα δεδομένα που διακινούνται μέσω απομακρυσμένης σύνδεσης, θα είναι κρυπτογραφημένα.

9.6.4.2.2. Η απομακρυσμένη σύνδεση θα καταγράφεται και η καταγραφή θα περιλαμβάνει:

- Ώρα έναρξης και λήξης της σύνδεσης
- Χρονική διάρκεια της σύνδεσης
- Σύστημα που αφορά η σύνδεση

9.6.4.3. Προστασία διαγνωστικών θυρών

Διαχείριση διαγνωστικών θυρών ή modems για την πρόσβαση τρίτων για διαγνωστικούς λόγους ή για συντήρηση λογισμικού.

9.6.4.3.1. Οι διαγνωστικές θύρες θα είναι απενεργοποιημένες.

9.6.4.3.2. Αν ζητηθεί από εξωτερικό συνεργάτη η ενεργοποίηση των διαγνωστικών θυρών, αυτό θα γίνεται από το ΤΠΟ και μόνο για το χρόνο που απαιτούν οι εργασίες που θα γίνουν.

9.6.4.4. Έλεγχοι σύνδεσης στο δίκτυο

Δημιουργία ομάδων χρηστών, υπηρεσιών και συστημάτων στο δίκτυο.

9.6.4.4.1. Μόνο εξουσιοδοτημένοι χρήστες θα συνδέονται στο δίκτυο.

9.6.4.4.2. Για την πρόσβαση των χρηστών στο δίκτυο του νοσοκομείου υπεύθυνο είναι το ΤΠΟ.

9.6.4.4.3. Νέοι χρήστες του δικτύου θα ενημερώνονται για τις υποχρεώσεις που απορρέουν από την Πολιτική Ασφάλειας του ΟΠΣΝ.

9.6.4.4.4. Θα διενεργούνται τακτικοί έλεγχοι διείσδυσης (penetration testing) για την αξιολόγηση της ασφάλειας του δικτύου.

9.6.4.5. Έλεγχοι δρομολόγησης

9.6.4.5.1. Θα χρησιμοποιούνται αναχώματα ασφάλειας (firewall) για το λογικό διαχωρισμό του εσωτερικού δικτύου από εξωτερικά δίκτυα.

9.6.4.5.2. Θα γίνει κατάτμηση του εσωτερικού δικτύου σε υποδίκτυα.

9.6.4.5.3. Οι διευθύνσεις του εσωτερικού δικτύου (IP address) δεν θα είναι προσβάσιμες και ανιχνεύσιμες από εξωτερικά δίκτυα.

9.6.5. Έλεγχος πρόσβασης στο λειτουργικό σύστημα

Διαδικασίες προστασίας του λειτουργικού συστήματος από μη εξουσιοδοτημένη πρόσβαση.

9.6.5.1. Διαδικασίες ασφαλής σύνδεσης

Έλεγχοι για την πρόσβαση εξουσιοδοτημένων χρηστών στα λειτουργικά συστήματα

9.6.5.1.1. Κάθε χρήστης έχει μοναδικό όνομα χρήστη και συνθηματικό.

9.6.5.1.2. Θα δημιουργηθεί «**Αρχείο Χρηστών**» και των αντίστοιχων Ονομάτων τους.

9.6.5.1.3. Ανενεργοί λογαριασμοί για περισσότερο από δύο (2) μήνες θα κλειδώνονται.

9.6.5.1.4. Ο χρόνος αδράνειας ενός σταθμού εργασίας θα είναι 15 λεπτά. Στο τέλος του χρόνου ο σταθμός εργασίας θα κλειδώνει.

9.6.5.1.5. Η πρόσβαση σε ανενεργό σταθμό θα γίνεται με εισαγωγή των συνθηματικών.

9.6.5.1.6. Αν οι χρήστες αφήνουν τη θέση εργασίας τους θα κλειδώνουν άμεσα τους σταθμούς εργασίας (με χρήση CTRL – ALT - DEL).

9.6.5.2. Ταυτοποίηση και αυθεντικοποίηση χρήστη

Προστασία κατά την απομακρυσμένη σύνδεση χρηστών.

9.6.5.2.1. Ο χρήστης θα χρησιμοποιεί το μοναδικό όνομα χρήστη και συνθηματικό για τη σύνδεση στο λειτουργικό.

9.6.5.1.2. Το πλήθος εσφαλμένων προσπαθειών σύνδεσης θα είναι πέντε (5).

9.6.5.3. Σύστημα διαχείρισης συνθηματικών

Θα χρησιμοποιείται το σύστημα διαχείρισης συνθηματικών του λειτουργικού του νοσοκομείου.

9.6.5.3.1. Το σύστημα διαχείρισης θα παραμετροποιηθεί έτσι ώστε να εξασφαλίζει τα απαιτούμενα μέτρα ασφάλειας.

9.6.6. Έλεγχος πρόσβασης στις εφαρμογές και τις πληροφορίες τους

Προστασία του λογισμικού εφαρμογών από μη εξουσιοδοτημένη πρόσβαση.

9.6.6.1. Περιορισμοί στην πρόσβαση των εφαρμογών

Η πρόσβαση σε πληροφορίες και λειτουργίες των εφαρμογών από τους χρήστες και το προσωπικό υποστήριξης θα πρέπει να περιορίζεται σύμφωνα με την καθορισμένη πολιτική πρόσβασης.

9.6.6.1.1. Κάθε εφαρμογή θα παρέχει στους χρήστες μόνο τις πληροφορίες που απαιτούνται από το ρόλο του χρήστη.

9.6.6.1.2. Οι χρήστες θα έχουν πρόσβαση μόνο στις διαδικασίες που απαιτούνται από το ρόλο του χρήστη.

9.6.6.2. Απομόνωση ευαίσθητων συστημάτων

Προστασία των κρίσιμων συστημάτων, Εξυπηρετητών, Βάσεων δεδομένων.

9.6.6.2.1. Οι εξυπηρετητές εφαρμογών θα είναι απομονωμένοι.

9.6.6.2.2. Οι κρίσιμες εφαρμογές θα φιλοξενούνται σε απομονωμένα υπολογιστικά συστήματα.

9.6.6.2.3. Δεν θα παρέχεται σε κανένα χρήστη η δυνατότητα της απευθείας διαχείρισης των εγγραφών της βάσης δεδομένων.

9.6.6.2.4. Τα υποσυστήματα που φιλοξενούν κρίσιμες εφαρμογές να επικοινωνούν μόνο με έμπιστα συστήματα και με ασφαλή τρόπο.

9.6.7. Έλεγχοι για φορητούς υπολογιστές και τηλεργασία

Διαδικασίες προστασίας στη χρήση φορητών υπολογιστών και τηλεργασίας.

9.6.7.1. Φορητοί υπολογιστές

9.6.7.1.1. Φορητοί υπολογιστές δεν θα χρησιμοποιούνται στο ΠΣ του νοσοκομείου.

9.6.7.1.2. Σε περίπτωση που κριθεί απαραίτητη χρήση φορητού υπολογιστή, θα ελέγχεται για το αν πληροί τις απαιτούμενες απαιτήσεις ασφάλειας.

9.7 Απόκτηση, Ανάπτυξη και Συντήρηση ΠΣ

Ασφάλεια στον κύκλο ζωής του ΠΣ.

9.7.1. Απαιτήσεις ασφάλειας ΠΣ

Οι ρυθμίσεις ασφαλείας που απαιτούνται για να διασφαλιστεί ότι η ασφάλεια αποτελεί αναπόσπαστο μέρος των συστημάτων.

9.7.1.1. Καθορισμός των απαιτήσεων ασφάλειας των ΠΣ

Οι ρυθμίσεις ασφαλείας που απαιτούνται για συγκεκριμένες υπηρεσίες, όπως χαρακτηριστικά ασφαλείας, τα επίπεδα εξυπηρέτησης και οι απαιτήσεις διαχείρισης.

9.7.1.1.1. Οι προδιαγραφές για το ΠΣ ή την εφαρμογή να περιλαμβάνει και ανάλυση επικινδυνότητας.

9.7.1.1.2. Η ανάπτυξη των εφαρμογών θα ακολουθεί συγκεκριμένες, επιστημονικά αποδεκτές μεθοδολογίες ανάπτυξης λογισμικού.

9.7.1.1.3. Η ανάπτυξη των ΠΣ θα γίνεται σε δοκιμαστικό περιβάλλον και μετά θα τίθεται σε παραγωγική λειτουργία.

9.7.1.1.4. Θα καταγράφονται όλες οι ενέργειες ανάπτυξης και συντήρησης του λογισμικού.

9.7.1.2. Εξασφάλιση σωστών διαδικασιών στις εφαρμογές

Οι ρυθμίσεις που απαιτούνται για να αποφευχθούν τα λάθη, η απώλεια, η μη εξουσιοδοτημένη τροποποίηση ή η κακή χρήση των πληροφοριών σε εφαρμογές.

9.7.1.2.1. Η εισαγωγή των δεδομένων σε εφαρμογές πρέπει να είναι επικυρωμένη για να διασφαλίζεται ότι τα δεδομένα είναι ορθά και ενδεδειγμένα.

9.7.1.2.2. Θα υπάρχει διαδικασία ελέγχου των δεδομένων που εισάγονται στο σύστημα.

Π.χ. να μην επιτρέπεται σε πεδίο για αριθμητικές τιμές να εισαχθούν αλφαβητικά ή αλφαριθμητικά δεδομένα.

9.7.1.2.3. Ο Υπεύθυνος Ασφάλειας θα εκτελεί δειγματοληπτικούς ελέγχους για την ακρίβεια των δεδομένων.

9.7.1.3. Έλεγχοι των διαδικασιών των εφαρμογών

Έλεγχοι επαλήθευσης πρέπει να ενσωματωθούν σε εφαρμογές για την ανίχνευση οποιασδήποτε αλλοίωσης της πληροφορίας μέσα από τα λάθη επεξεργασίας ή κάποιες σκόπιμες πράξεις.

9.7.1.3.1. Οι εφαρμογές θα ενσωματώνουν διαδικασίες ελέγχου και επαλήθευσης των πληροφοριών.

Π.χ. διαδικασία ελέγχου διπλοεγγραφών.

9.8 Διαχείριση Περιστατικών Ασφάλειας

Αντιμετώπιση των περιστατικών Ασφάλειας.

9.8.1. Αναφορά περιστατικών ασφάλειας και ευπαθειών

Να διασφαλιστεί ότι τα περιστατικά ασφάλειας και οι αδυναμίες που συνδέονται με τα συστήματα πληροφοριών γνωστοποιούνται με τρόπο που επιτρέπει έγκαιρες διορθωτικές ενέργειες που πρέπει να ληφθούν.

9.8.1.1. Αναφορά περιστατικών ασφάλειας

Τα συμβάντα ασφαλείας των πληροφοριών πρέπει να αναφέρονται μέσω των κατάλληλων διαδικασιών διαχείρισης όσο το δυνατόν ταχύτερα.

9.8.1.1.1. Όλα τα περιστατικά ασφάλειας θα πρέπει να αναφέρονται στον Υπεύθυνο Ασφάλειας του νοσοκομείου.

9.8.1.1.2. Θα δημιουργηθεί αρχείο «Περιστατικών Ασφάλειας» και φόρμα «Αναφοράς Περιστατικού Ασφάλειας».

Το αρχείο και η *φόρμα θα περιέχουν:*

- *Στοιχεία αυτού που κάνει την αναφορά*
- *Ημερομηνία και ώρα που συνέβη το περιστατικό*
- *Περιγραφή του περιστατικού*
- *Υπολογιστής/Σύστημα που έγινε το περιστατικό*
- *Διορθωτικές ενέργειες που έγιναν*

9.8.1.2. Αναφορά ευπαθειών του ΠΣ

Όλοι οι εργαζόμενοι, οι εργολάβοι και οι τρίτοι χρήστες των πληροφοριακών συστημάτων και υπηρεσιών υποχρεούνται να σημειώνουν και να αναφέρουν κάθε αδυναμία στην ασφάλεια που εντοπίσουν.

9.8.1.2.1. Όλοι οι υπάλληλοι του νοσοκομείου είναι υποχρεωμένοι να αναφέρουν σημεία ευπάθειας που εντοπίζουν στο ΠΣ.

9.8.1.2.2. Θα δημιουργηθεί φόρμα «Αναφοράς Ευπάθειας».

Η φόρμα θα περιέχει:

- *Στοιχεία αυτού που κάνει την αναφορά*
- *Ημερομηνία και ώρα που εντοπίστηκε*
- *Περιγραφή της ευπάθειας*
- *Υπολογιστής/Σύστημα που αφορά*
- *Διορθωτικές ενέργειες που έγιναν*

9.8.2. Διαχείριση των περιστατικών ασφάλειας και βελτιώσεις

Να εξασφαλιστεί η συνεπής και αποτελεσματική προσέγγιση που θα εφαρμόζεται για τη διαχείριση των περιστατικών ασφάλειας.

9.8.2.1. Ευθύνες και διαδικασίες

Οι αρμοδιότητες διαχείρισης και οι διαδικασίες θα πρέπει να θεσπιστούν για διασφαλίζουν την ταχεία, αποτελεσματική και ομαλή απόκριση σε περιστατικά παραβίασης της ασφαλείας.

9.8.2.1.1. Ο Υπεύθυνος Ασφάλειας είναι θα ερευνήσει το περιστατικό ασφάλειας.

9.8.2.1.2. Αρωγός του Υπεύθυνου Ασφάλειας είναι το ΤΠΟ.

9.8.2.1.3. Όλα τα περιστατικά παραβίασης θα ερευνούνται.

9.8.2.1.4. Θα εκτελούνται οι απαραίτητες ενέργειες για την αντιμετώπιση του περιστατικού.

9.8.2.1.5. Θα ελέγχονται όλα τα συστήματα που έχουν σχέση με το περιστατικό παραβίασης.

9.8.2.1.6. Θα ενημερώνεται το αρχείο «Περιστατικών Ασφάλειας»

9.8.2.2. Συλλογή αποδείξεων

Όταν μια δράση παρακολούθησης εναντίον ενός ατόμου ή οργανισμού μετά από ένα περιστατικό πληροφοριών ασφαλείας περιλαμβάνει νομική δράση (είτε αστικό ή ποινικό), θα πρέπει τα αποδεικτικά στοιχεία να συλλέγονται, να διατηρούνται, και να υποβάλλονται σε συμμόρφωση με τους κανόνες για τις ενδείξεις που προβλέπονται στη σχετική δικαιοδοσία (ες).

9.8.2.2.1. Θα συλλέγονται επαρκή αποδεικτικά στοιχεία να υποστηρίξουν νομικές ενέργειες κατά τρίτων.

9.8.2.2.2. Θα ζητείται η συμβολή της νομικής υπηρεσίας πριν από κάθε ενέργεια.

9.8.2.2.3. Θα ενημερώνονται οι αρμόδιες αρχές.

9.9 Διαχείριση Επιχειρησιακής Συνέχειας

Ασφάλεια πληροφοριών και επιχειρησιακή συνέχεια

9.9.1 Απαιτήσεις ασφάλειας πληροφοριών

Οι ρυθμίσεις ασφαλείας που απαιτούνται για συγκεκριμένες υπηρεσίες, όπως χαρακτηριστικά ασφαλείας, τα επίπεδα εξυπηρέτησης και οι απαιτήσεις διαχείρισης.

9.9.1.1. Εφεδρικά αντίγραφα

Θα τηρούνται αντίγραφα ηλεκτρονικών και μη δεδομένων

9.9.1.1.1. Θα υπάρχει εφεδρικό αντίγραφο δεδομένων.

9.9.1.1.2. Θα υπάρχει εφεδρικό αντίγραφο λογισμικού.

9.9.1.1.3. Θα υπάρχει αντίγραφο του «Αρχείου Χρηστών».

9.9.1.1.4. Θα υπάρχουν οδηγίες για την επαναφορά του ΠΣ.

9.9.1.2. Επιχειρησιακή συνέχεια και ανάλυση κινδύνου

Η στρατηγική για την επιχειρησιακή συνέχεια θα στηριχθεί στην εκτίμηση κινδύνου για τα αγαθά του νοσοκομείου.

9.9.1.1.1. Σημείο αναφορά του ΣΕΣ θα αποτελέσει η εκτίμηση κινδύνου.

9.9.1.3. Ανάπτυξη και εφαρμογή σχεδίου επιχειρηματικής συνέχειας

Θα πρέπει να αναπτυχθούν και να εφαρμοστούν τα σχέδια για τη διατήρηση ή την αποκατάσταση της λειτουργίας του ΠΣ στο απαιτούμενο επίπεδο και στο απαιτούμενο χρονικό διάστημα μετά από διακοπή ή βλάβη.

9.9.1.3.1. Θα υπάρχουν οδηγίες για την επαναφορά του ΠΣ.

9.9.1.3.2. Θα υπάρχει εφεδρικός εξυπηρετητής για τους κρίσιμους εξυπηρετητές.

9.9.1.3.3. Για τον κρίσιμο υλικό εξοπλισμό θα υπάρχουν συμβόλαια συντήρησης που προβλέπουν αντικατάσταση των συστημάτων σε χρονικό διάστημα μικρότερο των τριών (3) ημερών.

9.9.1.3.4. Τα συστήματα θα είναι απολύτως συμβατά με τα ήδη υπάρχοντα συστήματα.

9.9.1.3.5. Τα σχετικά συμβόλαια θα πρέπει να προβλέπουν ψηλές ρήτρες σε περίπτωση μη τήρησης των συμφωνηθέντων.

9.9.1.3.6. Θα εξασφαλιστεί κατάλληλος χώρος για την εγκατάσταση των εφεδρικών συστημάτων.

9.9.1.3.7. Ο εφεδρικός χώρος θα διαθέτει όλες τις απαιτούμενες εγκαταστάσεις ηλεκτρικής ενέργειας, δικτύωσης και τηλεπικοινωνιών.

9.9.1.3.8. Ο εφεδρικός χώρος θα ελέγχεται τακτικά.

9.9.1.4. Πλαίσιο σχεδιασμού της επιχειρηματικής συνέχειας

Θα πρέπει διατηρείται ένα ενιαίο πλαίσιο των σχεδίων για να εξασφαλίσει ότι όλα τα σχέδια είναι συνεπή, να αντιμετωπίζει με συνέπεια τις απαιτήσεις ασφάλειας των πληροφοριών, καθώς και για να καθοριστούν οι προτεραιότητες για τη δοκιμή και τη συντήρηση.

9.9.1.4.1. Το ΣΕΣ θα καλύπτει όλα τα υπάρχοντα υποσυστήματα.

9.9.1.4.2. Η ανάπτυξη νέων συστημάτων θα λαμβάνει υπόψη και την ανάγκη για επιχειρησιακή συνέχεια.

9.9.1.4.3. Το προσωπικό θα εκπαιδευτεί στην εφαρμογή του ΣΕΣ.

9.9.1.4. Έλεγχος, συντήρηση και επανεκτίμηση του σχεδίου της επιχειρηματικής συνέχειας

Τα σχέδια της επιχειρηματικής συνέχειας *θα πρέπει να ελέγχονται και να ενημερώνονται τακτικά για να είναι ενημερωμένα και αποτελεσματικά.*

9.9.1.4.1. Οι έλεγχοι που θα λάβουν χώρα κατά την εκτίμηση του ΣΕΣ να είναι σαφώς προσδιορισμένοι.

9.9.1.4.2. Το ΣΕΣ θα ανανεώνεται όταν υπάρχουν αλλαγές στο ΠΣ.

9.9.1.4.3. Το ΣΕΣ θα λαμβάνει υπόψη τα αποτελέσματα των ελέγχων και θα ανανεώνεται.

9.10 Συμμόρφωση

Έλεγχοι για τη συμμόρφωση των διαδικασιών του νοσοκομείου και των υπαλλήλων του με τις νομοθετικές, συμβατικές και κανονιστικές απαιτήσεις.

9.10.1. Συμμόρφωση με νομοθετικές απαιτήσεις

Για την αποφυγή οποιασδήποτε παραβίασης του νόμου, κανονιστικών ή συμβατικών υποχρεώσεων και των απαιτήσεων ασφάλειας.

9.10.1.1. Η επεξεργασία των δεδομένων υπόκειται στον Ν. 2472/97

9.10.1.2. Η επεξεργασία των δεδομένων στον τηλεπικοινωνιακό τομέα υπόκειται στον Ν. 2774/99

9.10.1.3. Η επεξεργασία των δεδομένων υπόκειται στις οδηγίες της ΑΠΔΠΧ.

9.10.1.4. Για την τήρηση αρχείου ευαίσθητων προσωπικών δεδομένων απαιτείται η άδεια της ΑΠΔΠΧ.

9.10.2. Δικαιώματα πνευματικής ιδιοκτησίας

Κατάλληλες διαδικασίες θα πρέπει να εφαρμοστούν για να εξασφαλιστεί η συμμόρφωση με τις νομοθετικές, κανονιστικές και συμβατικές απαιτήσεις για τη χρήση του υλικού σε σχέση με τις οποίες μπορεί να υπάρχουν δικαιώματα πνευματικής ιδιοκτησίας και για τη χρήση των ιδιόκτητων προϊόντων λογισμικού.

9.10.2.1. Η επεξεργασία Απαγορεύεται η εγκατάσταση προγραμμάτων στους σταθμούς εργασίας χωρίς την άδεια του ΤΠΟ.

9.10.2.2. Απαγορεύεται η εγκατάσταση προγραμμάτων χωρίς άδεια του κατασκευαστή τους.

Κεφάλαιο 10
Σχέδιο Ανάκαμψης από Καταστροφή

Σχέδιο για την αποκατάσταση της λειτουργίας του ΠΣ του «HOSPITAL» σε περίπτωση καταστροφής

10.1 Σκοπός του Σχεδίου Ανάκαμψης από Καταστροφή (Disaster Recovery Plan – DRP)

Ο κύριος στόχος του DRP είναι η αποκατάσταση και συνέχιση της λειτουργίας του νοσοκομείου, αν συμβεί μια καταστροφή.

10.2 Εύρος του Σχεδίου Ανάκαμψης από Καταστροφή

Το DRP αφορά στο ΟΠΣΝ του «HOSPITAL». Ένα μεγάλο μέρος της υλοποίησης του ΟΠΣΝ έχει γίνει κεντρικοποιημένα από την ΥΠε με αποτέλεσμα να υπάρχουν κοινά αγαθά μεταξύ του «HOSPITAL», των υπολοίπων νοσοκομείων που ανήκουν στην ΥΠε και της διοίκησης της ΥΠε. Αυτό σημαίνει ότι οι αρχές και τα μέτρα που θα προκύψουν από το DRP αφορά σε σημαντικό βαθμό και το ΟΠΣΥ.

Το χρονικό όριο που τίθεται για την ανάκαμψη του ΠΣ είναι τρεις (3) ημέρες.

Το DRP θα πρέπει να επαναξιολογείται και να αναθεωρείται αν υπάρξουν αλλαγές και τροποποιήσεις στο ΠΣ.

10.3 Μεθοδολογία του Σχεδίου Ανάκαμψης από Καταστροφή

Για την εκπόνηση του DRP κρίσιμο ρόλο παίζουν οι εξής παράγοντες:

1. Η ανάλυση κινδύνων για το ΟΠΣΝ

2. Η υφιστάμενη κατάσταση σχετικά με τις διαδικασίες που ακολουθούνται στο νοσοκομείο για την δημιουργία εφεδρικών αντιγράφων (Back up) του λογισμικού. Η λήψη αντιγράφων είναι απαραίτητη και κρίσιμη διαδικασία για την ανάκαμψη του ΠΣ, καθώς από αυτά θα επαναφέρουμε το ΠΣ στην πρότερη κατάσταση από την στιγμή της καταστροφής. Το Back up του νοσοκομείου υλοποιείται ως εξής:

    2.1. Τα εφεδρικά αντίγραφα παίρνονται καθημερινά στις 5:00 πμ. Αυτό σημαίνει ότι υπάρχει ένα κενό διάστημα από την στιγμή που θα ληφθούν τα αντίγραφα έως τη χρονική στιγμή της καταστροφής για το οποίο τα δεδομένα θα χαθούν.

2.2. Τα αντίγραφα αποθηκεύονται σε συστοιχίες δίσκων με την τεχνολογία RAID (Redundant Array of Indepent Disks).

2.3. Παίρνονται αντίγραφα ημερήσια, εβδομαδιαία και μηνιαία.

2.4. Λαμβάνεται backup των βάσεων δεδομένων, των εφαρμογών και των λειτουργικών συστημάτων των εξυπηρετητών.

2.5. Τα αντίγραφα αποθηκεύονται σε συστοιχίες δίσκων με την τεχνολογία RAID (Redundant Array of Indepent Disks).

3. Ο εξοπλισμός σε υλικό και λογισμικό του νοσοκομείου.

4. Τα κόστη των υπαρχουσών τεχνικών ανάκαμψης από καταστροφή.

Σύμφωνα με αυτό το πλαίσιο πρέπει να επισημάνουμε τα εξής:

1. Τα κρισιμότερα συστήματα, τα οποία πρέπει άμεσα να επανέλθουν σε παραγωγική διαδικασία είναι αυτά που χρησιμοποιούνται για την εξυπηρέτηση των ασθενών. Δηλαδή:

1.1. Υποσύστημα Διαχείρισης Ασθενών

1.2. Υποσύστημα Εργαστηρίων

1.3. Υποσύστημα Φαρμακείου

2. Τα υποσυστήματα Διοικητικού – Οικονομικού είναι λιγότερο κρίσιμα από ότι τα παραπάνω.

3. Παρόλο αυτά στην ανάλυση της αρχιτεκτονική του ΟΠΣΥ διαπιστώθηκε ότι τα Υποσυστήματα αυτά χρησιμοποιούν κοινούς πληροφοριακούς πόρους. Αυτό σημαίνει ότι θα πρέπει να ανακάμψουν ταυτόχρονα για να μπορούν να λειτουργήσουν.

Το νοσοκομείο θα χρειαστεί προσωρινές εγκαταστάσεις όπου θα εγκατασταθεί ο εφεδρικός εξοπλισμός. Οι προσωρινές εγκαταστάσεις μπορεί να είναι:

- Πλήρως εξοπλισμένοι χώροι, έτοιμοι προς άμεση λειτουργία (hot sites)
- Μερικώς εξοπλισμένοι χώροι (warm sites)
- Μη εξοπλισμένες εγκαταστάσεις με τηλεφωνική σύνδεση και παροχή ηλεκτρικού ρεύματος (cold sites)

- Κινητές εγκαταστάσεις (Mobile sites)
- Εγκαταστάσεις κλώνους της βασικής εγκατάστασης (Mirrored sites), οι οποίες αποτελούν και την πιο ακριβή λύση, αφού ουσιαστικά έχουμε ένα δεύτερο πανομοιότυπο ΠΣ, να δουλεύει ταυτόχρονα για την περίπτωση καταστροφής.

10.4 Στρατηγική του DRP για το ΟΠΣΝ

Διαδικασίες πριν και μετά την καταστροφή.

10.4.1 Προετοιμασία αντιμετώπισης της καταστροφής

Οι διαδικασίες που θα ακολουθηθούν και τα απαραίτητα μέτρα για την προετοιμασία αντιμετώπισης καταστροφής είναι τα εξής:

1. Θα καθοριστούν κριτήρια ενεργοποίησης του DRP. Η διαδικασία ανάκαμψης θα αποφασιστεί με βάση αυτά τα κριτήρια.
2. Θα καταγραφούν αναλυτικά οι οδηγίες του σχεδίου για ανάκαμψη από καταστροφή.
3. Θα οριστεί Υπεύθυνος Ανάκαμψης από καταστροφή.
4. Θα συσταθεί ομάδας ανάκαμψης από καταστροφή

    4.1. Η ομάδα ανάκαμψης θα αποτελείται από προσωπικό όλων των νοσοκομείων που ανήκουν στο ΟΠΣΥ και προσωπικό της διοίκησης της ΥΠε.

5. Η ομάδα ανάκαμψης θα έχει το απαραίτητο γνωστικό υπόβαθρο για την υλοποίηση του σχεδίου.
6. Η ομάδα ανάκαμψης θα εκπαιδευτεί κατάλληλα.
7. Θα καθοριστεί ο χώρος που θα χρησιμοποιηθεί για την εγκατάσταση του εφεδρικού εξοπλισμού.
8. Θα γίνει πλήρης καταγραφή του εξοπλισμού και του λογισμικού.

9. Θα υπάρχει πλάνο καταγραφής και συσχέτισης εξοπλισμού και λογισμικού.

10. Θα υπάρχει καταγραφή των λειτουργιών, ρυθμίσεων, διαμόρφωσης των μηχανημάτων.

11. Θα ελέγχονται και θα καταγράφονται όλες οι αλλαγές στο ΠΣ.

12. Θα υπάρχουν όλα τα εφεδρικά δεδομένα φυλαγμένα σε ασφαλή χώρο.

13. Μαζί με τα εφεδρικά δεδομένα θα υπάρχει το απαραίτητο λογισμικό, drivers, updates κλπ.

10.4.2 Διαδικασίες Ανάκαμψης

Στην περίπτωση που υπάρξει ένα περιστατικό που θα οδηγήσει σε καταστροφή του ΠΣ, θα πρέπει να γίνουν τα εξής:

1. Ενημέρωση και κλήση του Υπεύθυνου Ανάκαμψης

2. Ενημέρωση και κλήση των μελών της Ομάδας Ανάκαμψης από Καταστροφή

3. Έλεγχος των κριτηρίων ενεργοποίησης του σχεδίου.

    3.1. Την τελική απόφαση ενεργοποίησης του σχεδίου την έχει ο Διοικητής της ΥΠε.

    3.2. Ο Υπεύθυνος Ανάκαμψης θα ενημερώσει τον Διοικητή της ΥΠε.

Κεφάλαιο 11
Κώδικας Δεοντολογίας

Η σύνταξη του κώδικα δεοντολογίας είναι απαίτηση της ΑΠΔΠΧ.

11.1 Κώδικας Δεοντολογίας του «HOSPITAL»

Ο κώδικας ορίζει τους κανόνες που πρέπει να τηρούνται από το προσωπικό του νοσοκομείου που δεν δεσμεύεται από το ιατρικό απόρρητο, για την διατήρηση της εμπιστευτικότητας των ιατρικών δεδομένων.

11.1.1 Εισαγωγή

Ο κώδικας δεοντολογίας αναφέρεται στις απαραίτητες αρχές που πρέπει να τηρούνται από το προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας που δεν δεσμεύεται από το ιατρικό απόρρητο, ώστε να εξασφαλίζεται η προστασία των ιατρικών δεδομένων των ασθενών.

Ειδικότερα ο κώδικας δεοντολογίας αφορά το προσωπικό που χρησιμοποιεί τις εφαρμογές του νοσοκομείου οι οποίες διαχειρίζονται τα δεδομένα υγείας, όπως επίσης και το προσωπικό που είναι υπεύθυνο για τον σχεδιασμό, ανάπτυξη και συντήρηση αυτών των εφαρμογών.

Ο κώδικας δεν περιλαμβάνει τεχνικές λεπτομέρειες για την διατήρηση της εμπιστευτικότητας των ιατρικών δεδομένων αλλά ορίζει τους κανόνες που πρέπει να τηρούνται.

Η αποδοχή και τήρηση του κώδικα από το προσωπικό ανήκει στη Διοίκηση του Νοσοκομείου και στο ίδιο το προσωπικό.

Ενότητα 1: Πλαίσιο Αξιοποίησης

1.1. Βασικές Αρχές Δεοντολογίας

1.1.1. Αρχή του Αυτοπροσδιορισμού

Όλοι οι άνθρωποι έχουν το δικαίωμα του αυτοπροσδιορισμού.

1.1.2. Αρχή της ισότητας

Όλοι οι άνθρωποι είναι ίσοι μεταξύ τους και έχουν το δικαίωμα ανάλογης μεταχείρισης.

1.1.3. Αρχή της Αλληλεγγύης

Όλοι οι άνθρωποι οφείλουν να προάγουν το καλό των άλλων ατόμων, εφόσον η φύση των πράξεων τους βρίσκεται σε αρμονία με τις θεμελιώδεις αξίες των επηρεαζόμενων ατόμων.

1.1.4. Αρχή του Αλτρουισμού

Όλοι οι άνθρωποι οφείλουν να αποτρέπουν την πρόκληση βλάβης σε άλλους ανθρώπους, εφόσον μπορούν να το πράξουν χωρίς να προξενήσουν αδικαιολόγητη βλάβη στους εαυτούς τους ή σε τρίτους.

1.1.5. Αρχή της Εφικτότητας

Όλα τα δικαιώματα και οι υποχρεώσεις των ανθρώπων ισχύουν υπό την προϋπόθεση ότι είναι δυνατόν να πραγματοποιηθούν στις συγκυρίες που επικρατούν.

1.1.6. Αρχή της Βέλτιστης Προσπάθειας

Κάθε άνθρωπος που έχει μια υποχρέωση οφείλει να την εκπληρώσει όσο πιο καλά μπορεί.

1.2. Γενικές Αρχές Δεοντολογίας αρχές στις Τεχνολογίες Πληροφορικής και Επικοινωνιών

1.2.1. Αρχή της διαφύλαξης της Ιδιωτικότητας

Όλοι οι άνθρωποι έχουν το δικαίωμα της διαφύλαξης της ιδιωτικότητας και επομένως του ελέγχου της συλλογής, αποθήκευσης, πρόσβασης, χρήσης, μετάδοσης, μεταχείρισης και διάθεσης των προσωπικών τους δεδομένων.

1.2.2. Αρχή της ενημέρωσης

Η συλλογή, αποθήκευση, πρόσβαση, χρήση, μετάδοση, μεταχείριση και διάθεση προσωπικών δεδομένων πρέπει να γνωστοποιείται στο υποκείμενο των δεδομένων με κατάλληλο και έγκυρο τρόπο.

1.2.3. Αρχή της Αναλογικότητας

Τα προσωπικά δεδομένα που συλλέγονται νομίμως πρέπει να προστατεύονται με επαρκή και κατάλληλα μέτρα από απώλεια, μη εξουσιοδοτημένη καταστροφή, πρόσβαση, χρήση μετατροπή ή μετάδοση τους.

1.2.4. Αρχή της Επικαιρότητας

Το υποκείμενο ενός Ιατρικού Φακέλου έχει το δικαίωμα της πρόσβασης στο φάκελο αυτό καθώς και το δικαίωμα τροποποίησης του φακέλου για την αποκατάσταση της ακρίβειας, πληρότητας και συνάφειας των δεδομένων.

1.2.5. Αρχή του Ελέγχου

Το δικαίωμα ελέγχου της συλλογής, αποθήκευσης, πρόσβασης, χρήσης, μεταχείρισης, μετάδοσης και διάθεσης των προσωπικών δεδομένων περιορίζεται μόνο από νόμιμες, κατάλληλες και συναφείς πληροφοριακές ανάγκες, μια ελεύθερης, υπεύθυνης και δημοκρατικής κοινωνίας, καθώς και από τα ίσα και αντίστοιχα δικαιώματα άλλων ατόμων.

1.2.6. Αρχή της Ελάχιστης Βλάβης

Κάθε παραβίαση του δικαιώματος ιδιωτικότητας ενός ανεξάρτητου ατόμου και του δικαιώματος καθενός να ελέγχει τα σχετικά τα σχετικά με το άτομο του δεδομένα, όπως καθορίζονται από την *Αρχή της Ιδιωτικότητας,* μπορεί να λάβει χώρα μόνο με τρόπο που προσβάλλει ελάχιστα τα δικαιώματα του επηρεαζόμενου ατόμου.

1.2.7. Αρχή της Αιτιολόγησης

Κάθε παραβίαση του δικαιώματος διαφύλαξης της ιδιωτικότητας του ατόμου και του δικαιώματος ελέγχου των δεδομένων που σχετίζονται με αυτό πρέπει να αιτιολογείται στον επηρεαζόμενο, έγκαιρα και με κατάλληλο τρόπο.

Ενότητα 2: Κανόνες Δεοντολογικής Συμπεριφοράς των Υπεύθυνων Επεξεργασίας και του μη ιατρικού Προσωπικού Επεξεργασίας Προσωπικών Δεδομένων Υγείας

2.1. Καθήκοντα απέναντι στο Υποκείμενο

2.1.1. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να διασφαλίζει ότι τα πιθανά υποκείμενα των Πληροφοριών Υγείας Ασθενούς (πχ. ασθενής) είναι ενημερωμένα για την ύπαρξη συστημάτων, προγραμμάτων ή συσκευών των οποίων σκοπός είναι η συλλογή ή/και η μετάδοση δεδομένων που τα αφορούν.

2.1.2. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να διασφαλίσει ότι υπάρχουν κατάλληλες διαδικασίες, έτσι ώστε:

α. Οι Ιατρικοί Φάκελοι Ασθενών να δημιουργούνται και μεταδίδονται μόνο με την εκούσια, επαρκή και ρητή συγκατάθεση των υποκείμενων αυτών των φακέλων.

β. Αν ένας Ιατρικός Φάκελος Ασθενή δημιουργείται ή μεταδίδεται κατά παράβαση του Α.2.1, τότε η ανάγκη να δημιουργηθεί ή να μεταδοθεί έχει προκύψει με βάση ανεξάρτητη και σύμφωνη με τη δεοντολογία αιτιολόγηση, σε έγκαιρο χρόνο και με κατάλληλο τρόπο.

2.1.3. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να διασφαλίσει ότι το υποκείμενο ενός Ιατρικού Φακέλου Ασθενή έχει ενημερωθεί:

α. για το γεγονός ότι ο Ιατρικός Φάκελος Ασθενή έχει δημιουργηθεί για αυτόν,

β. για το ποιος έχει δημιουργήσει τον Ιατρικό Φάκελο Ασθενή και ποιος τον συντηρεί,

γ. για το τι περιέχεται στον Ιατρικό Φάκελο Ασθενή,

δ. για το σκοπό για τον οποίο έχει δημιουργηθεί ο Ιατρικός Φάκελος Ασθενή,

ε. για τα άτομα, οργανισμούς και υπηρεσίες που έχουν πρόσβαση στον Ιατρικό Φάκελο Ασθενή ή που μπορεί να μεταδοθεί ο Ιατρικός Φάκελος Ασθενή ή ένα επεξεργάσιμο μέρος του.

στ. για το που τηρείται ο Ιατρικός Φάκελος Ασθενή,

ζ. για το χρονικό διάστημα για το οποίο θα διατηρηθεί,

η. για την τελική μορφή του Ιατρικού Φακέλου Ασθενή,

θ. για την προέλευση των δεδομένων που περιέχονται στο φάκελο,

ι. για τα δικαιώματα που έχει σε σχέση με την πρόσβαση, χρήση αποθήκευση, μετάδοση, διαχείριση, ποιότητα, διόρθωση και διάθεση του Ιατρικού Φακέλου Ασθενή καθώς και των δεδομένων που περιέχονται σε αυτόν.

2.1.4. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να διασφαλίζει ότι:

α. οι Ιατρικοί Φάκελοι Ασθενή αποθηκεύονται, προσπελαύνονται, χρησιμοποιούνται, τροποποιούνται ή μεταδίδονται μόνο για νόμιμους σκοπούς,

β. υπάρχουν εγκατεστημένα κατάλληλα πρωτόκολλα και μηχανισμοί που μπορούν να παρακολουθούν την αποθήκευση, πρόσβαση, χρήση τροποποίηση ή μετάδοση των Ιατρικών Φακέλων Ασθενή ή των δεδομένων που περιέχονται σε αυτούς, όπως ορίζει ο κανόνας Α.2.1,

γ. τα υποκείμενα των Ιατρικών Φακέλων Ασθενή γνωρίζουν την ύπαρξη των ανωτέρω πρωτοκόλλων και μηχανισμών,

δ. τα υποκείμενα των Ιατρικών Φακέλων Ασθενή διαθέτουν κατάλληλα μέσα, ώστε να μπορούν να θέτουν ερωτήματα και να συμμετάσχουν στην εφαρμογή των σχετικών πρωτοκόλλων και μηχανισμών εποπτείας.

2.1.5. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας αναγνωρίζει ότι τα υποκείμενα των Ιατρικών Φακέλων Ασθενή και οι νόμιμοι αντιπρόσωποι τους έχουν τα ίδια δικαιώματα με το Προσωπικό του νοσοκομείου στους Ιατρικούς Φάκελους Ασθενή που τα αφορούν καθώς και ότι το δικαίωμα αυτό το γνωρίζουν στα υποκείμενα.

2.1.6. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να διασφαλίσει ότι οι Ιατρικοί Φάκελοι Ασθενή υφίστανται δίκαιη, έντιμη και σύννομη επεξεργασία.

2.1.7. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να διασφαλίσει ότι έχουν ληφθεί τα απαραίτητα μέτρα που παρέχουν επαρκή ασφάλεια, ποιότητα, ευχρηστία και προσβασιμότητα.

2.1.8. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να διασφαλίσει, στο μέτρο των δυνατοτήτων του, ότι ένας Ιατρικός Φάκελος Ασθενή ή τα δεδομένα που περιέχονται σε αυτόν χρησιμοποιούνται μόνο για τους δηλωθέντες σκοπούς για τους οποίους συλλέχθηκαν ή για σκοπούς οι οποίοι είναι δεοντολογικά αποδεκτοί.

2.1.9. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να διασφαλίσει ότι τα υποκείμενα των Ιατρικών Φακέλων Ασθενή ή των σχετικών επικοινωνιών καθίστανται ενήμερα των πιθανών παραβιάσεων και των αιτιών που τις προκάλεσαν.

2.2.Καθήκοντα απέναντι στο Ιατρικό Προσωπικό

2.2.1. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει:

α. να βοηθά το αρμόδιο Ιατρικό Προσωπικό που ασχολείται με την περίθαλψη των ασθενών, παρέχοντας του κατάλληλη, έγκαιρη και ασφαλή πρόσβαση σε σχετικούς Ιατρικούς Φακέλους Ασθενή (ή μέρη αυτών),

β. να διασφαλίσει τη χρηστικότητα, ακεραιότητα και την υψηλότερη δυνατή τεχνική ποιότητα των Ιατρικών Φακέλων Ασθενή,

γ. να παρέχει τις πληροφοριακές υπηρεσίες που είναι απαραίτητες στο Ιατρικό Προσωπικό για την εκπλήρωση των καθηκόντων του.

2.2.2. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να τηρεί το Ιατρικό Προσωπικό ενήμερο για την κατάσταση των πληροφοριακών υπηρεσιών τις οποίες χρησιμοποιεί ο Ιατρικός Φάκελος Ασθενή και να το ενημερώνει έγκαιρα για οποιοδήποτε πρόβλημα ή δυσκολία που μπορεί να σχετίζεται ή που μπορούσε λογικά να προκύψει σε σχέση με τις υπηρεσίες αυτές.

2.2.3. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να ενημερώνει το Ιατρικό Προσωπικό με το οποίο συνεργάζεται επαγγελματικά ή στο οποίο παρέχει επαγγελματικές υπηρεσίες για οποιεσδήποτε συνθήκες που μπορούν να επηρεάσουν την αντικειμενικότητα των συμβούλων που παρέχει το Ιατρικό Προσωπικό ή που μπορούν να βλάψουν τη φύση ή την ποιότητα των υπηρεσιών που παρέχουν στο Ιατρικό Προσωπικό.

2.2.4. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να διασφαλίζει την ύπαρξη περιβάλλοντος που συμβάλλει στη διατήρηση των υψηλότερων δυνατών προδιαγραφών για τη συλλογή, αποθήκευση, διαχείριση, μετάδοση και χρήση δεδομένων από το Ιατρικό Προσωπικό για παροχή ιατρικής περίθαλψης.

2.2.5. Το Ιατρικό Προσωπικό που εμπλέκεται άμεσα με στη δημιουργία Ιατρικών Φακέλων Ασθενή ενδέχεται να έχει δικαιώματα πνευματικής ιδιοκτησίας σε συγκεκριμένα τμήματα των φακέλων αυτών. Συνεπώς, το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να προστατεύει τόσο τον Ιατρικό Φάκελο Ασθενή, όσο και το σύστημα συλλογής, ανάκτησης,

αποθήκευσης και χρήσης των δεδομένων, όπου είναι ενσωματωμένος ο Ιατρικός Φάκελος Ασθενή.

2.3 Καθήκοντα απέναντι στο Νοσοκομείο

2.3.1. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να επιδεικνύει, έναντι του Νοσοκομείου, εργατικότητα, ακεραιότητα και εύλογη αφοσίωση.

2.3.2. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να:

α. επιδεικνύει ευαισθησία σε θέματα ασφάλειας, σύμφωνα με τη δεοντολογία και το γενικότερο πλαίσιο του οργανισμού στον οποίο ασκεί το επάγγελμα του,

β. διευκολύνει το σχεδιασμό και την υλοποίηση των βέλτιστων δυνατών και πιο κατάλληλων τεχνικών και οργανωτικών μέτρων ασφαλείας των δεδομένων,

γ. υλοποιήσει και να διατηρήσει τα υψηλότερα δυνατά ποιοτικά πρότυπα συλλογής, αποθήκευσης, ανάκτησης, επεξεργασίας, πρόσβασης, μετάδοσης και χρήσης δεδομένων.

2.3.3. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να διασφαλίσει, στο μέγιστο δυνατό βαθμό, ότι υπάρχουν οι απαραίτητες υποδομές για την τεχνική, νομική και δεοντολογική αποδοχή της συλλογής, αποθήκευσης, ανάκτησης, επεξεργασίας, πρόσβασης, μετάδοσης και χρήσης δεδομένων.

2.3.4. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να ειδοποιήσει, έγκαιρα και με κατάλληλο τρόπο, τους αρμοδίους στο Νοσοκομείο, σε θέματα ασφάλειας συστημάτων, προγραμμάτων, συσκευών ή διαδικασιών δημιουργίας, αποθήκευσης, πρόσβασης, χειρισμού και μετάδοσης του οργανισμού, με τον οποίο έχει επαγγελματικούς δεσμούς ή των εργοδοτών για τους οποίους παρέχει επαγγελματικές υπηρεσίες, για κάθε περιστατικό παραβίασης.

2.3.5. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να ενημερώνει, έγκαιρα και με κατάλληλο τρόπο, το Νοσοκομείο για κάθε πρόβλημα ή δυσκολία που θα μπορούσε να ανακύψει και να επηρεάσει την απόδοση των παρεχόμενων υπηρεσιών προς αυτούς.

2.3.6. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να ενημερώνει έγκαιρα το Νοσοκομείο για τις συνθήκες που θα μπορούσαν να επηρεάσουν την αντικειμενικότητα των υπηρεσιών που παρέχει.

2.3.7. Για την εκτέλεση των καθηκόντων του, το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να χρησιμοποιεί εργαλεία, τεχνικές και συσκευές που έχουν αποκτηθεί σύμφωνα με το νόμο και τη δεοντολογία.

2.3.8. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να υποστηρίζει την ανάπτυξη και παροχή εκπαιδευτικών υπηρεσιών, σχετικών με τις Τεχνολογίες Πληροφορικής και Επικοινωνιών, στο Νοσοκομείο.

2.4 Καθήκοντα απέναντι στο Κοινωνικό Σύνολο

2.4.1. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να διευκολύνει τη συλλογή, αποθήκευση, μετάδοση και χρήση των δεδομένων υγείας, τα οποία είναι απαραίτητα για το σχεδιασμό και την παροχή υπηρεσιών ιατρικής περίθαλψης του κοινωνικού συνόλου.

2.4.2. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να διασφαλίσει ότι:

α. συλλέγονται μόνο δεδομένα που αφορούν έννομες ανάγκες,

β. τα δεδομένα τα οποία συλλέγονται είναι μη αναγνωρίσιμα ή καθίστανται ανώνυμα στο μέγιστο δυνατό βαθμό, σύμφωνα με τους νόμιμους σκοπούς συλλογής τους,

γ. η διασύνδεση βάσεων δεδομένων γίνεται μόνο για νόμιμους και δικαιολογημένους σκοπούς που δεν παραβιάζουν τα θεμελιώδη δικαιώματα των υποκειμένων ΗΦΥ,

δ. μόνο κατάλληλα εξουσιοδοτημένα άτομα έχουν πρόσβαση στα δεδομένα.

2.4.3. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να ενημερώσει το κοινό για τη φύση, συλλογή, αποθήκευση και χρήση των δεδομένων υγείας και να καθιστά το κοινωνικό σύνολο ενήμερο των προβλημάτων, κινδύνων, επιπτώσεων ή περιορισμών που λογικά θα μπορούσαν α συσχετιστούν με τη συλλογή, αποθήκευση, χρήση και μεταχείριση των δεδομένων αυτών.

2.4.4. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να αρνηθεί να συμμετάσχει ή να υποστηρίξει πρακτικές που παραβιάζουν τα ανθρώπινα δικαιώματα και τις ατομικές ελευθερίες.

2.5 Αυτοέλεγχος και αυτογνωσία

2.5.1. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να:

α. αναγνωρίσει τα όρια των αρμοδιοτήτων του,

β. διαβουλεύεται όταν είναι αναγκαίο η σκόπιμο,

γ. διατηρεί την επιστημονική του επάρκεια,

δ. αναλαμβάνει την ευθύνη για ενέργειες που εκτελεί ή βρίσκονται στον έλεγχο του,

ε. αποφεύγει διαπλοκή συμφερόντων,

στ. αναγνωρίζει ηθικά ή με το άλλο κατάλληλο τρόπο την εκτέλεση μιας εργασίας,

ζ. ενεργεί με εντιμότητα και ακεραιότητα.

2.6 Καθήκοντα απέναντι στο επάγγελμα

2.6.1. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να ενεργεί με τρόπο που δεν δυσφημεί το επάγγελμα του.

2.6.2. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να βοηθά την ανάπτυξη των υψηλότερων δυνατών προτύπων επαγγελματικής ικανότητας, να διασφαλίζει ότι τα πρότυπα αυτά είναι δημόσια γνωστά και να επιβλέπει ότι εφαρμόζονται με αμερόληπτο και διαφανή τρόπο.

2.6.3. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να αποφεύγει την αμφισβήτηση της φήμης των συνεργατών του, άλλα και να συνεργάζεται με τις αρμόδιες αρχές σε θέματα που αφορούν τυχόν αντιεπαγγελματική συμπεριφορά συνεργατών του.

2.6.4. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να βοηθά τους συνεργάτες του να ενεργούν με τρόπο αντάξιο των υψηλότερων τεχνικών και δεοντολογικών προτύπων του επαγγέλματος.

2.6.5. Το Προσωπικό Επεξεργασίας Προσωπικών Δεδομένων Υγείας οφείλει να προωθεί την κατάλληλη και δεοντολογικά αποδεκτή κατανόηση των δυνατοτήτων που προκύπτουν από την αποτελεσματικά χρήση των ΤΠΕ.

Βιβλιογραφία

[01] A. Calder, S. Watkins, "IT GOVERNANCE, A Manager's Guide to Data Security and ISO27001/ISO27002", 4η έκδοση, COGAN PAGE, 2008

[02] Τόκης Ι, Τόκη Ε, "Πληροφορική Υγείας", Εκδόσεις Τζιόλα, 2006

[03] Σ. Κάτσικας, Δ. Γκρίτζαλης, Σ. Γκρίτζαλης, "Ασφάλεια Πληροφοριακών Συστημάτων", Εκδόσεις Νέων Τεχνολογιών, 2004

[04] http://www.idika.gr/files/deltiatypou/deltio_typou_10_01.13_v2.pdf (21/1/12)

[05] http://www.syzefxis.gov.gr/

[06] http://www.himss.org/ASP/topics_ehr.asp

[07] http://www.yyka.gov.gr/articles/hlektronikes-efarmoges-e-s-y/831-hlektronikos-fakelos- asthenwn (13/1/13)

[08] http://www.yyka.gov.gr/articles/hlektronikes-efarmoges-e-s-y/830-mhxanografika-systhmata-nosokomeiwn (13/1/13)

[09] http://www.apollo.gr/dev/Orion/Rhapsody.asp 20/1/21013

[10] Πρόγραμμα Διαύγεια, ΑΔΑ Β44ΥΘ-2ΒΗ, http://et.diavgeia.gov.gr/f/yyka/ada/%CE%9244%CE%A5%CE%98-2%CE%92%CE%97 (13/1/13)

[11] Ν. Μανιαδάκης, Αλήθειες και Μύθοι για τα ΚΕΝ, (http://www.insuranceworld.gr/default.php?pname=Article&art_id=6861&cat_id=4 (13/1/13))

[12] Διαδικτυακή Εφαρμογή Εύρεσης ΚΕΝ, Εγχειρίδιο Χρήσης ver. 4.0, (30/9/11)

[13] http://www.healthcareinfosecurity.com/whitepapers/focus-on-prevention-best-remedy-for-medical-record-breaches-w-683 (17/3/2013)

[14] http://www.worldprivacyforum.org

[15] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html (16/3/13)

[16] MassDevice staff, http://www.massdevice.com/news/hackers-holding-hospital-records-hostage-officials-say, (16/3/13)

[17] http://www.fastcompany.com/3000470/medical-cybercrime-next-frontier (16/3/13)

[18] http://www.skai.gr/news/greece/article/193528/antigrafotouneo-htupima-apo-tous-anonymus-hackers/#ixzz2L5Lt43WM (03/02/2012)

[19] ictplus.gr (9/1/213)

[20] http://www.inews.gr/142/prostima-gia-paraviasi-prosopikon-dedomenon.htm (9/5/11)

[21] http://www.27000.org/index.htm

[22] Εθνικό Σχέδιο Δράσης για την Υγεία 2008 – 2012

[23] R. Cavali, J. Stevens, L. Young, W. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process", Carnegie Mellon, May 2007

Παράρτημα Α
Υλοποίηση OCTAVE Allegro

Οι διαδικασίες διαχείρισης επικινδυνότητας της μεθόδου OCTAVE Allegro.

Α.1 Φύλλα Εργασίας Μεθόδου OCTAVE Allegro

Παρουσίαση των συμπληρωμένων φύλλων εργασίας της μεθόδου κατά την διαχείριση της επικινδυνότητας.

Allegro Worksheet 1	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ **ΦΗΜΗ ΚΑΙ ΕΜΠΙΣΤΟΣΥΝΗ ΠΕΛΑΤΩΝ**		
Πεδίο Επιπτώσεων	**Χαμηλό**	**Μέτριο**	**Υψηλό**
Φήμη στο Ιατρικό-Νοσηλευτικό Προσωπικό	Η φήμη επηρεάζεται ελάχιστα, δεν υπάρχουν ενέργειες ή κόστη αποκατάστασης.	Η φήμη επηρεάστηκε και χρειάζονται ενέργειες και κόστη αποκατάστασης.	Η φήμη επηρεάστηκε ανεπανόρθωτα.
Φήμη στο μη Ιατρικό-Νοσηλευτικό Προσωπικό	Η φήμη επηρεάζεται ελάχιστα, δεν υπάρχουν ενέργειες ή κόστη αποκατάστασης.	Η φήμη επηρεάστηκε και χρειάζονται ενέργειες και κόστη αποκατάστασης.	Η φήμη επηρεάστηκε ανεπανόρθωτα.
Άλλο: Φήμη στους πολίτες	Η φήμη επηρεάζεται ελάχιστα, δεν υπάρχουν ενέργειες ή κόστη αποκατάστασης.	Η φήμη επηρεάστηκε και χρειάζονται ενέργειες και κόστη	Η φήμη επηρεάστηκε ανεπανόρθωτα.
Άλλο: Πληρότητα κρεβατιών	Ελάχιστα επηρεάστηκε η πληρότητα κρεβατιών.	Η πληρότητα έπεσε κατά <5%.	Μεγάλη μείωση της πληρότητας κατά >5%.

Allegro Worksheet 2	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ **ΟΙΚΟΝΟΜΙΚΑ**		
Πεδίο Επιπτώσεων	**Χαμηλό**	**Μέτριο**	**Υψηλό**
Λειτουργικά Κόστη	Ετήσια Αύξηση < 0,5%	Ετήσια Αύξηση από 0,5% έως 1%	Ετήσια Αύξηση > 1%
Μείωση εσόδων	Ετήσια Μείωση < 0,5%	Ετήσια Μείωση από 0,5% έως 1%	Ετήσια Μείωση > 1%
Στιγμιαία Οικονομική Απώλεια	<10.000 €	από 10.001% έως 50.000%	> 50.000 €

Allegro Worksheet 3	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ **ΠΑΡΑΓΩΓΙΚΟΤΗΤΑ**		
Πεδίο Επιπτώσεων	**Χαμηλό**	**Μέτριο**	**Υψηλό**
Εργατοώρες προσωπικού	Αύξηση εργατο-ωρών με κόστος < 5.000 €	Αύξηση εργατο-ωρών με κόστος από 5.001€ έως 10.000€	Αύξηση εργατο-ωρών με κόστος > 10.000 €
Άλλο: Κάλυψη Κρεβατιών	Μείωση < 2%.	Μείωση μεταξύ 2% και 5%	Μείωση > 5%
Άλλο: Επισκέπτες ΤΕΠ - ΑΙ - ΤΕΙ	Μείωση < 2%.	Μείωση μεταξύ 2% και 5%	Μείωση > 5%

Allegro Worksheet 4	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ **ΑΣΦΑΛΕΙΑ ΚΑΙ ΥΓΕΙΑ**		
Πεδίο Επιπτώσεων	**Χαμηλό**	**Μέτριο**	**Υψηλό**
Ζωή (Ασθενείς)	Δεν υπάρχει σημαντική απειλή η απώλεια στη ζωή ασθενή. Δεν λαμβάνονται ρυθμιστικά μέτρα.	Απειλούνται ζωές ασθενών, αλλά είναι ιάσιμη η βλάβη. Χρειάζονται να ληφθούν ελάχιστα ρυθμιστικά μέτρα κόστους <100.000€.	Απώλεια ασθενή. Σημαντικά ρυθμιστικά μέτρα πρέπει να ληφθούν, κόστους >100.000€.
Υγεία (Ασθενείς)	Ελάχιστη άμεσα ιάσιμη υποβάθμιση της υγείας ασθενή. Ελάχιστα ρυθμιστικά μέτρα πρέπει να ληφθούν κόστους <50.000€.	Προσωρινή ή θεραπεύσιμη βλάβη στην υγεία ασθενών. Χρειάζονται να ληφθούν ελάχιστα ρυθμιστικά μέτρα κόστους από 50.001€ έως 100.000€.	Μόνιμη βλάβη στην υγεία ασθενών. Σημαντικά ρυθμιστικά μέτρα πρέπει να ληφθούν, κόστους > 100.000€.

Ασφάλεια (Ασθενείς)	Υπάρχουν αμφιβολίες για την ασφάλεια. Ελάχιστα ή καθόλου μέτρα πρέπει να ληφθούν μηδενικού ή ελάχιστου κόστους.	Η ασφάλεια επηρεάζεται. Χρειάζονται να ληφθούν ελάχιστα ρυθμιστικά μέτρα κόστους <100.000€.	Η ασφάλεια παραβιάστηκε. Σημαντικά ρυθμιστικά μέτρα πρέπει να ληφθούν, κόστους >100.000€.
Ζωή (Προσωπικό)	Δεν υπάρχει σημαντική απειλή η απώλεια στη ζωή εργαζομένων. Δεν λαμβάνονται ρυθμιστικά μέτρα.	Απειλούνται ζωές εργαζομένων, αλλά είναι ιάσιμη η βλάβη. Χρειάζονται ελάχιστα ρυθμιστικά μέτρα κόστους <100.000€.	Απώλεια εργαζόμενου. Σημαντικά ρυθμιστικά μέτρα πρέπει να ληφθούν, κόστους >100.000€.
Υγεία (Προσωπικό)	Ελάχιστη άμεσα ιάσιμη υποβάθμιση της υγείας εργαζομένων. Ελάχιστα μέτρα πρέπει να ληφθούν κόστους < 50.000€.	Προσωρινή ή θεραπεύσιμη βλάβη στην υγεία εργαζομένων. Χρειάζονται ελάχιστα μέτρα κόστους από 50.001€ έως 100.000€.	Μόνιμη βλάβη στην υγεία εργαζομένων. Σημαντικά ρυθμιστικά μέτρα πρέπει να ληφθούν, κόστους > 100.000€.
Ασφάλεια (Προσωπικό)	Υπάρχουν αμφιβολίες για την ασφάλεια. Ελάχιστα ή καθόλου ρυθμιστικά μέτρα πρέπει να ληφθούν μηδενικού ή ελάχιστου κόστους.	Η ασφάλεια επηρεάζεται. Χρειάζονται να ληφθούν ελάχιστα ρυθμιστικά μέτρα κόστους < 100.000€.	Η ασφάλεια παραβιάστηκε. Σημαντικά ρυθμιστικά μέτρα πρέπει να ληφθούν, κόστους > 100.000€.

Allegro Worksheet 5	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ **ΠΡΟΣΤΙΜΑ ΚΑΙ ΝΟΜΙΚΕΣ ΚΥΡΩΣΕΙΣ**		
Πεδίο Επιπτώσεων	**Χαμηλό**	**Μέτριο**	**Υψηλό**
Πρόστιμα	Επιβολή προστίμου < 50.000€.	Επιβολή προστίμου από 50.000€ έως 100.000€.	Επιβολή προστίμου >100.000€.
Μηνύσεις	Αβάσιμες μηνύσεις ή μηνύσεις κατά του νοσοκομείου < 50.000€	Μηνύσεις κατά του νοσοκομείου από 50.000€ έως 100.000€	Μηνύσεις κατά του νοσοκομείου >100.000€
Έρευνες - Έλεγχοι	Καμία έρευνα – έλεγχος.	Έρευνα – έλεγχος κυβερνητικός ή άλλου οργανισμού απαιτεί πληροφορίες ή αρχεία (low profile).	Έρευνα – έλεγχος κυβερνητικός ή άλλου οργανισμού γίνεται σε βάθος.

Allegro Worksheet 7	ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ **ΤΑΞΙΝΟΜΗΣΗΣ ΠΕΔΙΩΝ ΕΠΙΠΤΩΣΕΩΝ**
ΤΑΞΙΝΟΜΗΣΗ	**ΠΕΔΙΟ ΕΠΙΠΤΩΣΕΩΝ**
4	**Φήμη και Εμπιστοσύνη Πελατών**
2	**Οικονομικά**
3	**Παραγωγικότητα**
5	**Ασφάλεια και Υγεία**
1	**Πρόστιμα και Νομικές Κυρώσεις**

Allegro Worksheet 8	ΠΡΟΦΙΛ ΚΡΙΣΙΜΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ (IT) A	
(1) Κρίσιμο Αγαθό: *Ποιο είναι το κρίσιμο IT αγαθό;*	**(2) Αιτιολόγηση της Επιλογής:** *Γιατί το IT αγαθό είναι σημαντικό για τον οργανισμό;*	**(3) Περιγραφή:** *Ποια είναι η συμφωνημένη περιγραφή του IT αγαθού;*
Δημογραφικά Δεδομένα Ασθενή - ΔΔΑ	Α. Είναι συστατικό στοιχείο του ΗΦΑ Β. Είναι απαραίτητα για τη διαχείριση του ασθενή στις διαδικασίες του νοσοκομείου Γ. Είναι ευαίσθητα προσωπικά δεδομένα	Δημογραφικά δεδομένα: Στοιχεία ασθενή, ονοματεπώνυμο, πατρώνυμο, δ/νση, τηλέφωνα, ασφαλιστικά στοιχεία. Μέρος των δημογραφικών δεδομένων εκτός της ηλεκτρονικής μορφής εκτυπώνονται στα: - Εισιτήρια – εξιτήρια - Απαιτήσεις σε ασφαλιστικά ταμεία - Τιμολόγια – αποδείξεις - Ιατρικές βεβαιώσεις - Χειρόγραφο Φάκελο Ασθενή - Απαντήσεις Εργαστηρίων Το αγαθό είναι απαραίτητο για όλες τις διαδικασίες που αφορούν στη διαχείριση του ασθενή. Συγκεκριμένα χρειάζεται στις διαδικασίες των: - Γρ. Κίνησης - Κλινικών - Γραμματεία Ε.Ι. – Α.Ι. – Τ.Ε.Π. - Φαρμακείο - Λογιστήριο Ασθενών - Εργαστήρια
(4) Ιδιοκτήτης/τες: *Σε ποιους ανήκει το IT αγαθό;*		
- Γρ. Κίνησης - Κλινικές - Γραμματεία Ε.Ι. – Α.Ι. – Τ.Ε.Π. - Φαρμακείο - Λογιστήριο Ασθενών - Εργαστήρια		
(5) Απαιτήσεις Ασφάλειας: *Ποιες είναι οι απαιτήσεις ασφάλειας για το IT αγαθό;*		
❑ **Εμπιστευτικότητα (Confidentiality)**	Μόνο εξουσιοδοτημένο προσωπικό του νοσοκομείου μπορεί να δει το αγαθό ως εξής:	Τα ΔΔΑ μπορεί να δει το προσωπικό των τμημάτων: - Γρ. Κίνησης - Κλινικές - Γραμματεία Ε.Ι. – Α.Ι. – Τ.Ε.Π. - Φαρμακείο - Λογιστήριο Ασθενών - Τ.Π.Ο. - Εργαστήρια
	Μόνο εξουσιοδοτημένο προσωπικό των παρόχων μπορεί να δει το αγαθό ως εξής:	Τα ΔΔΑ μπορεί να δει το προσωπικό των παρόχων: - Πάροχος Υποσυστήματος Διαχείρισης Ασθενή - Πάροχος Π.Σ. Εργαστηρίων

❑ **Ακεραιότητα (Integrity)**	Μόνο εξουσιοδοτημένο προσωπικό του νοσοκομείου μπορεί να τροποποιήσει το αγαθό ως εξής:	Η διαχείριση των ΔΔΑ (Εισαγωγή, Διαγραφή, Τροποποίηση) θα γίνεται από εξουσιοδοτημένο προσωπικό των τμημάτων: - Γρ. Κίνησης - Κλινικές - Γραμματεία Ε.Ι. – Α.Ι. – Τ.Ε.Π. - Λογιστήριο Ασθενών - Τ.Π.Ο.
	Μόνο εξουσιοδοτημένο προσωπικό του παρόχου μπορεί να τροποποιήσει το αγαθό ως εξής:	Η διαχείριση των ΔΔΑ (Εισαγωγή, Διαγραφή, Τροποποίηση) μπορεί να γίνει από εξουσιοδοτημένο προσωπικό των παρόχων: - Πάροχος Υποσυστήματος Διαχείρισης Ασθενή
❑ **Διαθεσιμότητα (Availability)**	Το εξουσιοδοτημένο προσωπικό πρέπει να έχει πρόσβαση το αγαθό ως εξής:	Τα ΔΔΑ πρέπει να είναι διαθέσιμα στα παρακάτω τμήματα για τις ημέρες λειτουργίας τους: - Γρ. Κίνησης - Κλινικές - Γραμματεία Ε.Ι. – Α.Ι. – Τ.Ε.Π. - Φαρμακείο - Λογιστήριο Ασθενών - Τ.Π.Ο. - Εργαστήρια
	Το αγαθό πρέπει να είναι διαθέσιμο για **24** ώρες, **7** μέρες/εβδομάδα, **52** εβδομάδες/χρόνο.	Το ΔΔΑ πρέπει να είναι διαθέσιμο κατά τη διάρκεια λειτουργίας των τμημάτων που το χρησιμοποιούν. Στις Κλινικές και τα Εργαστήρια που δουλεύουν 24 ώρες θα πρέπει να είναι διαθέσιμο όλο το 24ωρο.
❑ **Άλλο**	Το αγαθό υπόκειται σε νόμους για την ασφάλεια ως εξής:	Τα ΔΔΑ περιέχουν πληροφορίες οι οποίες είναι εμπιστευτικές όπως Αριθμό Μητρώου, Αρ. Ταυτότητας, τηλέφωνο κλπ.

(6) Σημαντικότερες Απαιτήσεις Ασφάλειας: *Ποιες είναι οι σημαντικότερες απαιτήσεις ασφάλειας για το IT αγαθό;*

✓ Εμπιστευτικότητα	❑ Ακεραιότητα	❑ Διαθεσιμότητα	❑ Άλλο

Allegro Worksheet 9a	**ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (ΤΕΧΝΙΚΟ)**
ΕΣΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**
Υποσύστημα Διαχείρισης Ασθενών και Εργαστηρίων του ΚΔΝ. Αποτελείται από: α) Συστοιχία (cluster) δύο servers β) Βάση δεδομένων Microsoft SQL 2000 γ) Εφαρμογή Διαχείρισης Ασθενή.	Τ.Π.Ο.
Δίκτυο του Νοσοκομείου, μέσω του οποίου μεταδίδονται τα δεδομένα.	Τ.Π.Ο.
Σταθμοί Εργασίας του Νοσοκομείου.	Τ.Π.Ο. Χρήστης Σταθμού Εργασίας
ΕΞΩΤΕΡΙΚΟ	
Περιγραφη Περιεκτη	Ιδιοκτητησ(τεσ)
Internet. Αποστολή μέσω διαδικτύου απαιτήσεων σε ασφαλιστικά ταμεία.	Ασφαλιστικά ταμεία

Allegro Worksheet 9b	ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (Φυσικο)
ΕΣΩΤΕΡΙΚΟ	
Περιγραφη Περιεκτη	Ιδιοκτητησ(τεσ)
Χειρόγραφος Φάκελος Ασθενή	Γρ. Κίνησης
	Τ.Ε.Ι. – Α.Ι. – Τ.Ε.Π.
	Κλινικές
Εισιτήριο – Εξιτήριο, τιμολόγια ασθενή, απαιτήσεις από ασφαλιστικά ταμεία	Τμήματα έκδοσης αντίστοιχων παραστατικών
Αντίγραφα ασφάλειας σε κασέτα	Τ.Π.Ο.
ΕΞΩΤΕΡΙΚΟ	
Περιγραφη Περιεκτη	Ιδιοκτητησ(τεσ)
Αντίγραφα σε χαρτί των πληροφοριών δίνονται στους ασθενείς	Ασθενείς
Αντίγραφα σε χαρτί των πληροφοριών δίνονται στα Ασφαλιστικά ταμεία	Ασφαλιστικά ταμεία

Allegro Worksheet 9c	ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (ΑΝΘΡΩΠΟΙ)
ΕΣΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΟΝΟΜΑ Ή ΡΟΛΟΣ/ΑΡΜΟΔΙΟΤΗΤΑ	**ΤΜΗΜΑ/ΜΟΝΑΔΑ**
Προσωπικό Γρ. Κίνησης	Γρ. Κίνησης
Προσωπικό Τ.Ε.Ι. – Α.Ι. - Τ.Ε.Π.	Τ.Ε.Ι. – Α.Ι. – Τ.Ε.Π.
Ιατρικό – Νοσηλευτικό Προσωπικό	Κλινικές
Προσωπικό Φαρμακείου	Φαρμακείο
Προσωπικό Λογιστηρίου Ασθενών	Λογιστήριο Ασθενών
Προσωπικό Τ.Π.Ο.	Τ.Π.Ο.
ΕΞΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΑΝΑΔΟΧΟΣ, ΠΡΟΜΗΘΕΥΤΗΣ, ΚΛΠ.	**ΟΡΓΑΝΙΣΜΟΣ**
Προσωπικό Παρόχου Υποσυστήματος Διαχείρισης Ασθενή	Πάροχος Υποσυστήματος Διαχείρισης Ασθενή
Προσωπικό Υ.ΠΕ.	Υ.ΠΕ.
Προσωπικό Ασφαλιστικών Ταμείων	Ασφαλιστικά Ταμεία

Allegro Worksheet 10		ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ	
Information Asset Risk	Threat	**IT Αγαθό**	***Δημογραφικά Δεδομένα Ασθενή***
		Πεδίο Προσοχής	***Αστοχία Υλικού***
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	
		(3) Κίνητρο: *Γιατί το κάνει;*	
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες

		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*			**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*	
				Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
	Η απώλεια Διαθεσιμότητας των ΔΔΑ επιφέρει σοβαρά προβλήματα δυσλειτουργίας στο νοσοκομείο, αφού είναι απαραίτητα για τη διαχείριση του ασθενή. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα.			Φήμη και εμπιστοσύνη πελατών (4)	3	12
				Οικονομικά (2)	1	2
				Παραγωγικότητα (3)	2	6
				Ασφάλεια και Υγεία (5)	1	5
				Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
					Relative Risk Score	**26**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εξυπηρετητές	Συμβόλαιο συντήρησης Παρακολούθηση Αντίγραφα Ασφάλειας Χρήση σύμφωνη με τις προδιαγραφές του κατασκευαστή
Βάση δεδομένων	Συμβόλαιο συντήρησης Αντίγραφα Ασφάλειας
Σταθμοί εργασίας	Συμβόλαιο συντήρησης Παρακολούθηση Χρήση σύμφωνη με τις προδιαγραφές του κατασκευαστή
Δίκτυο Νοσοκομείου	Συμβόλαιο Συντήρησης Παρακολούθηση Σωστή χρήση

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**	
Information Asset Risk	**Threat**	**IT Αγαθό**	***Δημογραφικά Δεδομένα Ασθενή***
		Πεδίο Προσοχής	***Φυσική Καταστροφή***
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	

		(3) Κίνητρο: *Γιατί το κάνει;*			
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη**	**Καταστροφή**	
			Τροποποίηση	**Διακοπή**	
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η απώλεια Διαθεσιμότητας των ΔΔΑ επιφέρει σοβαρά προβλήματα δυσλειτουργίας στο νοσοκομείο, αφού είναι απαραίτητα για τη διαχείριση του ασθενή. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα.	Φήμη και εμπιστοσύνη πελατών (4)	3	12
	Οικονομικά (2)	1	2
	Παραγωγικότητα (3)	2	6
	Ασφάλεια και Υγεία (5)	1	5
	Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
	Relative Risk Score		**26**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Δωμάτιο εξυπηρετητών	Έλεγχοι προστασίας από φυσικές καταστροφές Έλεγχοι προστασίας από διακοπή ηλεκτροδότησης Μέτρα ασφάλειας για πλημμύρα και πυρκαγιά
Εξυπηρετητές	Συμβόλαιο συντήρησης Σχέδιο Ανάκαμψης από Καταστροφή
Βάση δεδομένων	Συμβόλαιο συντήρησης Αντίγραφα Ασφάλειας
Δίκτυο Νοσοκομείου	Έλεγχοι προστασίας από φυσικές καταστροφές Έλεγχοι προστασίας από διακοπή ηλεκτροδότησης Συμβόλαιο Συντήρησης

	Allegro Worksheet 10	***Κίνδυνος για το IT Αγαθο***
	IT Αγαθό:	***Δημογραφικά Δεδομένα Ασθενή***
Information Asset Risk	**Πεδίο Προσοχής**	***Αστοχία Λογισμικού***

		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*			
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*			
		(3) Κίνητρο: *Γιατί το κάνει;*			
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η απώλεια Διαθεσιμότητας των ΔΔΑ επιφέρει σοβαρά προβλήματα δυσλειτουργίας στο νοσοκομείο, αφού είναι απαραίτητα για τη διαχείριση του ασθενή. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα.	Φήμη και εμπιστοσύνη πελατών (4)	2	8
	Οικονομικά (2)	1	2
	Παραγωγικότητα (3)	3	9
	Ασφάλεια και Υγεία (5)	-	-
	Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
		Relative Risk Score	**20**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Λογισμικό Εφαρμογών – Εξυπηρετητών – Βάσεις δεδομένων	Έλεγχος αλλαγών Συμβόλαιο συντήρησης Αντίγραφα Ασφάλειας

	Allegro Worksheet 10	***Κίνδυνος για το IT Αγαθο***		
	IT Αγαθό	***Δημογραφικά Δεδομένα Ασθενή***		
Information Asset Risk	**Threat**	**Πεδίο Προσοχής**	***Σκόπιμη Βλάβη στο Υλικό***	
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	Υπάλληλος του νοσοκομείου ή τρίτος	

		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	Πρέπει να αποκτήσει πρόσβαση στους χώρους του νοσοκομείου όπου υπάρχει εξοπλισμός του ΠΣ.		
		(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος		
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
		Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η απώλεια Διαθεσιμότητας των ΔΔΑ επιφέρει σοβαρά προβλήματα δυσλειτουργίας στο νοσοκομείο, αφού είναι απαραίτητα για τη διαχείριση του ασθενή. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα.		Φήμη και εμπιστοσύνη πελατών (4)	3	12
		Οικονομικά (2)	1	2
		Παραγωγικότητα (3)	2	6
		Ασφάλεια και Υγεία (5)	1	5
		Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
			Relative Risk Score	**26**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Δωμάτιο εξυπηρετητών	Έλεγχος φυσικής πρόσβασης Συμβόλαιο Συντήρησης
Δίκτυο Νοσοκομείου	Έλεγχος φυσικής πρόσβασης Συμβόλαιο Συντήρησης
Σταθμοί Εργασίας	Έλεγχος φυσικής πρόσβασης Συμβόλαιο συντήρησης

	Allegro Worksheet 10	***Κίνδυνος για το IT Αγαθο***	
	IT Αγαθό	***Δημογραφικά Δεδομένα Ασθενή***	
Information Asset Risk	**Threat**	**Πεδίο Προσοχής**	***Μη εξουσιοδοτημένη πρόσβαση στο Υποσύστημα Διαχείρισης Ασθενή***
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	1. Εσωτερικός χρήστης που έχει υποκλέψει συνθηματικά 2. Εξωτερικός χρήστης που έχει αποκτήσει πρόσβαση μέσω του

			δικτύου και έχει ανακαλύψει συνθηματικά			
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	1. Ο εσωτερικός χρήστης εκμεταλλευόμενος αμέλεια στη φύλαξη των συνθηματικών ενός νόμιμου χρήστη 2. Ο εξωτερικός χρήστης εκμεταλλευόμενος αδυναμία στην ασφάλεια του δικτύου			
		(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος			
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη**	**Καταστροφή**		
			Τροποποίηση	**Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Απώλεια Εμπιστευτικότητας και Ακεραιότητας			
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**	

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η μη εξουσιοδοτημένη πρόσβαση μπορεί να προκαλέσει απώλεια Εμπιστευτικότητας και Ακεραιότητας των ΔΔΑ. Η αποκάλυψη των δεδομένων των ασθενών θα επιφέρει σοβαρά προβλήματα αξιοπιστίας στο νοσοκομείο.	Φήμη και εμπιστοσύνη πελατών (4)	3	12
	Οικονομικά (2)	3	6
	Παραγωγικότητα (3)	3	9
	Ασφάλεια και Υγεία (5)	-	-
	Πρόστιμα και Νομικές Κυρώσεις (1)	3	3
	Relative Risk Score		**30**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εξυπηρετητές	Έλεγχος πρόσβασης Αυθεντικοποίηση χρηστών Παρακολούθηση τρίτων που έχουν πρόσβαση Συμβόλαιο συντήρησης
Βάση δεδομένων	Πρόσβασης μόνο μέσω της εφαρμογής Αυθεντικοποίηση χρηστών Παρακολούθηση τρίτων που έχουν πρόσβαση Συμβόλαιο συντήρησης Αντίγραφα Ασφάλειας
Δίκτυο Νοσοκομείου, ΚΥ	Έλεγχοι διείσδυσης (penetration testing) Εγκατάσταση αναχωμάτων ασφάλειας (firewalls)
Σταθμοί Εργασίας	Αυθεντικοποίηση χρηστών στο λειτουργικό και στις εφαρμογές

	Ενεργοποίηση οθόνης αδράνειας

		IT Αγαθό	***Δημογραφικά Δεδομένα Ασθενή***		
Information Asset Risk	**Threat**	**Πεδίο Προσοχής**	***Μη εξουσιοδοτημένη πρόσβαση στα Φυσικά Μέσα***		
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	Ο δράστης μπορεί να είναι εσωτερικός ή εξωτερικός		
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	Κάποιος που αποκτά πρόσβαση στους χώρους που φυλάσσονται τα φυσικά μέσα εκμεταλλευόμενος ανεπαρκή προστασία των χώρων ή αμέλεια του χρήστη που τα διαχειρίζεται.		
		(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος		
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Επηρεάζεται η Εμπιστευτικότητα του αγαθού		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
		(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*	
				Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
		Η μη εξουσιοδοτημένη πρόσβαση μπορεί να προκαλέσει απώλεια Εμπιστευτικότητας. Η αποκάλυψη των δεδομένων των ασθενών θα επιφέρει σοβαρά προβλήματα αξιοπιστίας στο νοσοκομείο.		Φήμη και εμπιστοσύνη πελατών (4)	3	12
				Οικονομικά (2)	3	6
				Παραγωγικότητα (3)	3	9
				Ασφάλεια και Υγεία (5)	-	-
				Πρόστιμα και Νομικές Κυρώσεις (1)	3	3
					Relative Risk Score	**30**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Φάκελοι Ασθενών και άλλα έγγραφα	Φύλαξη σε ασφαλή χώρο Οι υπάλληλοι θα παίρνουν τα απαραίτητα μέτρα ασφάλειας των εγγράφων
Αντίγραφα δεδομένων	Φύλαξη σε ασφαλή χώρο

Allegro Worksheet 10			***Κίνδυνος για το IT Αγαθο***			
		IT Αγαθό	***Δημογραφικά Δεδομένα Ασθενή***			
nformation Asset Risk	**Threat**	**Πεδίο Προσοχής**	***Ακούσιο Λάθος Εξουσιοδοτημένου Χρήστη***			
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	1. Εξουσιοδοτημένος χρήστης			
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*				
		(3) Κίνητρο: *Γιατί το κάνει;*	Ακούσια			
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**			
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Επηρεάζεται η Ακεραιότητα των αγαθών			
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**	
		(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
				Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
		Η λανθασμένη εισαγωγή δεδομένων θα προκαλέσει απώλεια της Ακεραιότητας των ΔΔΑ. Τα λάθη αυτά δεν επιφέρουν σοβαρά προβλήματα και μπορούν να διορθωθούν όταν ανακαλυφθούν.		Φήμη και εμπιστοσύνη πελατών (4)	2	8
				Οικονομικά (2)	1	2
				Παραγωγικότητα (3)	1	3
				Ασφάλεια και Υγεία (5)	1	5
				Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
					Relative Risk Score	**19**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αποδοχή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εφαρμογή	Η εφαρμογή θα έχει διαδικασίες ελέγχου εισαγωγής δεδομένων

	Η εφαρμογή θα έχει διαδικασίες ελέγχου διπλοεγγραφών

Allegro Worksheet 8	ΠΡΟΦΙΛ ΚΡΙΣΙΜΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΑΓΑΘΩΝ	
(1) Κρίσιμο Αγαθό: *Ποιο είναι το κρίσιμο IT αγαθό;*	**(2) Αιτιολόγηση της Επιλογής:** *Γιατί το IT αγαθό είναι σημαντικό για τον οργανισμό;*	**(3) Περιγραφή:** *Ποια είναι η συμφωνημένη περιγραφή του IT αγαθού;*
Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή - ΙΝΔΑ	Α. Είναι συστατικό στοιχείο του ΗΦΑ Β. Είναι απαραίτητα για τη διαχείριση του ασθενή στα Ιατρικά/Νοσηλευτικά τμήματα (κλινικές – εργαστήρια – ιατρεία) του νοσοκομείου Γ. Εμπίπτουν στο Ιατρικό Απόρρητο	ΙΝΔΑ: Ιατρικές πράξεις, νοσηλείες, ασθένειες, θεραπείες, έκβαση, εξετάσεις, αποτελέσματα. Συστατικά των ΙΝΔΑ εκτός της ηλεκτρονικής μορφής εκτυπώνονται στα: - Εισιτήρια – εξιτήρια - Απαιτήσεις σε ασφαλιστικά ταμεία - Ιατρικές βεβαιώσεις - Χειρόγραφο Φάκελο Ασθενή - Απαντήσεις Εργαστηρίων Το αγαθό χρειάζεται στις διαδικασίες των: - Γρ. Κίνησης - Κλινικών - Γραμματεία Ε.Ι. – Α.Ι. – Τ.Ε.Π. - Φαρμακείο - Λογιστήριο Ασθενών - Εργαστήρια
(4) Ιδιοκτήτης/τες: *Σε ποιους ανήκει το IT αγαθό;*		
- Γρ. Κίνησης - Κλινικές - Γραμματεία Ε.Ι. – Α.Ι. – Τ.Ε.Π. - Φαρμακείο - Λογιστήριο Ασθενών - Εργαστήρια		
(5) Απαιτήσεις Ασφάλειας: *Ποιες είναι οι απαιτήσεις ασφάλειας για το IT αγαθό;*		
❑ **Εμπιστευτικότητα (Confidentiality)**	Μόνο εξουσιοδοτημένο προσωπικό του νοσοκομείου μπορεί να δει το αγαθό ως εξής:	Τα ΙΝΔΑ ή μέρος αυτών, μπορεί να δει το προσωπικό των τμημάτων: - Γρ. Κίνησης - Κλινικές - Γραμματεία Ε.Ι. – Α.Ι. – Τ.Ε.Π. - Φαρμακείο - Λογιστήριο Ασθενών - Τ.Π.Ο. - Εργαστήρια

	Μόνο εξουσιοδοτημένο προσωπικό των παρόχων μπορεί να δει το αγαθό ως εξής:	Τα ΙΝΔΑ ή μέρος αυτών μπορεί να δει το προσωπικό των παρόχων: - Πάροχος Υποσυστήματος Διαχείρισης Ασθενή - Πάροχος Ιατρικού – Νοσηλευτικού Υποσυστήματος - Πάροχος Π.Σ. Εργαστηρίων
Ακεραιότητα (Integrity)	Μόνο εξουσιοδοτημένο προσωπικό του νοσοκομείου μπορεί να τροποποιήσει το αγαθό ως εξής:	Η διαχείριση των ΙΝΔΑ ή μέρος αυτών (Εισαγωγή, Διαγραφή, Τροποποίηση) μπορεί να γίνει από το εξουσιοδοτημένο προσωπικό των τμημάτων: - Γρ. Κίνησης - Κλινικές - Γραμματεία Ε.Ι. – Α.Ι. – Τ.Ε.Π. - Εργαστήρια - Τ.Π.Ο.
	Μόνο εξουσιοδοτημένο προσωπικό του παρόχου μπορεί να τροποποιήσει το αγαθό ως εξής:	Η διαχείριση των ΙΝΔΑ (Εισαγωγή, Διαγραφή, Τροποποίηση) μπορεί να γίνει από εξουσιοδοτημένο προσωπικό των παρόχων: - Πάροχος Υποσυστήματος Διαχείρισης Ασθενή - Πάροχος Υποσυστήματος Εργαστηρίων
Διαθεσιμότητα (Availability)	Το εξουσιοδοτημένο προσωπικό πρέπει να έχει πρόσβαση το αγαθό ως εξής:	Τα ΙΝΔΑ πρέπει να είναι διαθέσιμα στα παρακάτω τμήματα για τις ημέρες λειτουργίας τους: - Γρ. Κίνησης - Κλινικές - Γραμματεία Ε.Ι. – Α.Ι. – Τ.Ε.Π. - Φαρμακείο - Λογιστήριο Ασθενών - Τ.Π.Ο. - Εργαστήρια
	Το αγαθό πρέπει να είναι διαθέσιμο για **24** ώρες, **7** μέρες/εβδομάδα, **52** εβδομάδες/χρόνο.	Το ΙΝΔΑ πρέπει να είναι διαθέσιμο κατά τη διάρκεια λειτουργίας των τμημάτων που το χρησιμοποιούν. Στις Κλινικές και τα Εργαστήρια που δουλεύουν 24 ώρες θα πρέπει να είναι διαθέσιμο όλο το 24ωρο.
Άλλο	Το αγαθό υπόκειται σε νόμους για την ασφάλεια ως εξής:	Τα ΙΝΔΑ προστατεύονται από το Ιατρικό Απόρρητο.

(6) Σημαντικότερες Απαιτήσεις Ασφάλειας: *Ποιες είναι οι σημαντικότερες απαιτήσεις ασφάλειας για το ΙΤ αγαθό;*

Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα	Άλλο

Allegro Worksheet 9a	**ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ ΙΤ ΑΓΑΘΟΥ (ΤΕΧΝΙΚΟ)**
ΕΣΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**
Υποσύστημα Διαχείρισης Ασθενών και Εργαστηρίων του ΚΔΝ. Αποτελείται από: α) Συστοιχία (cluster) δύο servers β) Βάση δεδομένων Microsoft SQL 2000 γ) Εφαρμογή Διαχείρισης Ασθενή.	Τ.Π.Ο.
Δίκτυο του Νοσοκομείου, μέσω του οποίου μεταδίδονται τα δεδομένα.	Τ.Π.Ο.
Σταθμοί Εργασίας του Νοσοκομείου.	Τ.Π.Ο. Χρήστης Σταθμού Εργασίας
ΕΞΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**
Internet. Αποστολή μέσω διαδικτύου απαιτήσεων σε ασφαλιστικά ταμεία.	Ασφαλιστικά ταμεία

Allegro Worksheet 9b	**ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ ΙΤ ΑΓΑΘΟΥ (ΦΥΣΙΚΟ)**

ΕΣΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**
Χειρόγραφος Φάκελος Ασθενή	Γρ. Κίνησης
	Τ.Ε.Ι. – Α.Ι. – Τ.Ε.Π.
	Κλινικές
Εισιτήριο – Εξιτήριο, τιμολόγια ασθενή, απαιτήσεις από ασφαλιστικά ταμεία	Τμήματα έκδοσης αντίστοιχων παραστατικών
Αντίγραφα ασφάλειας σε κασέτα	Τ.Π.Ο.
ΕΞΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**
Αντίγραφα σε χαρτί των πληροφοριών δίνονται στους ασθενείς	Ασθενείς
Αντίγραφα σε χαρτί των πληροφοριών δίνονται στα Ασφαλιστικά ταμεία	Ασφαλιστικά ταμεία

Allegro Worksheet 9c	ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ ΙΤ ΑΓΑΘΟΥ (ΑΝΘΡΩΠΟΙ)
ΕΣΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΟΝΟΜΑ Ή ΡΟΛΟΣ/ΑΡΜΟΔΙΟΤΗΤΑ	**ΤΜΗΜΑ/ΜΟΝΑΔΑ**
Προσωπικό Γρ. Κίνησης	Γρ. Κίνησης
Προσωπικό Τ.Ε.Ι. – Α.Ι. - Τ.Ε.Π.	Τ.Ε.Ι. – Α.Ι. – Τ.Ε.Π.
Ιατρικό – Νοσηλευτικό Προσωπικό	Κλινικές
Προσωπικό Φαρμακείου	Φαρμακείο
Προσωπικό Λογιστηρίου Ασθενών	Λογιστήριο Ασθενών
Προσωπικό Τ.Π.Ο.	Τ.Π.Ο.
ΕΞΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΑΝΑΔΟΧΟΣ, ΠΡΟΜΗΘΕΥΤΗΣ, ΚΛΠ.	**ΟΡΓΑΝΙΣΜΟΣ**
Προσωπικό Παρόχου Υποσυστήματος Διαχείρισης Ασθενή	Πάροχος Υποσυστήματος Διαχείρισης Ασθενή
Προσωπικό Υ.ΠΕ.	Υ.ΠΕ.
Προσωπικό Ασφαλιστικών Ταμείων	Ασφαλιστικά Ταμεία

Allegro Worksheet 10		ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ ΙΤ ΑΓΑΘΟ	
Information Asset Risk	**Threat**	**IT Αγαθό**	***Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή - ΙΝΔΑ***
		Πεδίο Προσοχής	***Αστοχία Υλικού***
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	
		(3) Κίνητρο: *Γιατί το κάνει;*	

		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** Καταστροφή **Τροποποίηση** Διακοπή		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
		(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
			Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
		Η απώλεια Διαθεσιμότητας των ΙΝΔΑ επιφέρει σοβαρά προβλήματα δυσλειτουργίας στο νοσοκομείο, αφού είναι απαραίτητα για τη διαχείριση του διαδικασιών θεραπευτικής φροντίδας του ασθενή. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα.	Φήμη και εμπιστοσύνη πελατών (4)	3	12
			Οικονομικά (2)	1	2
			Παραγωγικότητα (3)	3	9
			Ασφάλεια και Υγεία (5)	1	5
			Πρόστιμα και Νομικές Κυρώσεις (1)	2	2
				Relative Risk Score	**30**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εξυπηρετητές	Συμβόλαιο συντήρησης Σχέδιο Ανάκαμψης από Καταστροφής
Βάση δεδομένων	Συμβόλαιο συντήρησης Αντίγραφα Ασφάλειας
Δίκτυο Νοσοκομείου	Συμβόλαιο Συντήρησης

		Allegro Worksheet 10	***Κίνδυνος για το IT Αγαθο***
		IT Αγαθό	***Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή - ΙΝΔΑ***
Information Asset Risk	**Threat**	**Πεδίο Προσοχής**	***Αστοχία Λογισμικού***
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	
		(3) Κίνητρο: *Γιατί το κάνει;*	

		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη**	**Καταστροφή**	
			Τροποποίηση	**Διακοπή**	
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
			Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
	Η απώλεια Διαθεσιμότητας των ΔΔΑ επιφέρει σοβαρά προβλήματα δυσλειτουργίας στο νοσοκομείο, αφού είναι απαραίτητα για τη διαχείριση του ασθενή. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα.		Φήμη και εμπιστοσύνη πελατών (4)	2	8
			Οικονομικά (2)	1	2
			Παραγωγικότητα (3)	3	9
			Ασφάλεια και Υγεία (5)	1	5
			Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
				Relative Risk Score	**25**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Λογισμικό Εφαρμογών – Εξυπηρετητών – Βάσεις δεδομένων	Έλεγχος αλλαγών Συμβόλαιο συντήρησης Αντίγραφα Ασφάλειας

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**		
Information Asset Risk	**Threat**	**IT Αγαθό**	***Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή - ΙΝΔΑ***	
		Πεδίο Προσοχής	***Φυσική Καταστροφή***	
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*		
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*		
		(3) Κίνητρο: *Γιατί το κάνει;*		
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη**	**Καταστροφή**
			Τροποποίηση	**Διακοπή**
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες	

		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*			**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*	
				Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
	Η απώλεια Διαθεσιμότητας των ΙΝΔΑ επιφέρει σοβαρά προβλήματα δυσλειτουργίας στο νοσοκομείο, αφού είναι απαραίτητα για τη διαχείριση του διαδικασιών θεραπευτικής φροντίδας του ασθενή. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα.			Φήμη και εμπιστοσύνη πελατών (4)	3	12
				Οικονομικά (2)	1	2
				Παραγωγικότητα (3)	3	9
				Ασφάλεια και Υγεία (5)	1	5
				Πρόστιμα και Νομικές Κυρώσεις (1)	2	2
					Relative Risk Score	**30**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Δωμάτιο εξυπηρετητών	Έλεγχοι προστασίας από φυσικές καταστροφές
Εξυπηρετητές	Συμβόλαιο συντήρησης Σχέδιο Ανάκαμψης από Καταστροφής
Βάση δεδομένων	Συμβόλαιο συντήρησης Αντίγραφα Ασφάλειας
Δίκτυο Νοσοκομείου	Έλεγχοι προστασίας από φυσικές καταστροφές Έλεγχοι προστασίας από διακοπή ηλεκτροδότησης Συμβόλαιο Συντήρησης

Allegro Worksheet 10	**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**		
		IT Αγαθό	***Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή - ΙΝΔΑ***
Information Asset Risk	**Threat**	**Πεδίο Προσοχής**	***<u>Μη εξουσιοδοτημένη πρόσβαση στο Υποσύστημα Διαχείρισης Ασθενή</u>***
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	1. Εσωτερικός χρήστης που έχει υποκλέψει συνθηματικά 2. Εξωτερικός χρήστης που έχει αποκτήσει πρόσβαση μέσω του δικτύου και έχει ανακαλύψει συνθηματικά
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	1. Ο εσωτερικός χρήστης εκμεταλλευόμενος αμέλεια στη φύλαξη των συνθηματικών ενός νόμιμου χρήστη 2. Ο εξωτερικός χρήστης εκμεταλλευόμενος αδυναμία στην ασφάλεια του δικτύου
		(3) Κίνητρο: *Γιατί το κάνει;*	1. Προσωπικό όφελος

			2. Ευχαρίστηση		
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Απώλεια Εμπιστευτικότητας και Ακεραιότητας		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η μη εξουσιοδοτημένη πρόσβαση μπορεί να προκαλέσει απώλεια Εμπιστευτικότητας και Ακεραιότητας των ΙΝΔΑ. Η αποκάλυψη των δεδομένων των ασθενών θα επιφέρει σοβαρά προβλήματα αξιοπιστίας στο νοσοκομείο.	Φήμη και εμπιστοσύνη πελατών (4)	3	12
	Οικονομικά (2)	3	6
	Παραγωγικότητα (3)	3	9
	Ασφάλεια και Υγεία (5)	-	-
	Πρόστιμα και Νομικές Κυρώσεις (1)	3	3
	Relative Risk Score		**30**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εξυπηρετητές	Έλεγχος πρόσβασης Παρακολούθηση τρίτων που έχουν πρόσβαση Συμβόλαιο συντήρησης
Βάση δεδομένων	Πρόσβαση μόνο μέσω της εφαρμογής Παρακολούθηση τρίτων που έχουν πρόσβαση Συμβόλαιο συντήρησης Αντίγραφα Ασφάλειας
Δίκτυο Νοσοκομείου, ΚΥ	Έλεγχοι διείσδυσης (penetration testing) Εγκατάσταση αναχωμάτων ασφάλειας (firewalls)
Σταθμοί Εργασίας	Αυθεντικοποίηση χρηστών στο λειτουργικό και στις εφαρμογές Ενεργοποίηση οθόνης αδράνειας

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**
	IT Αγαθό	***Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή - ΙΝΔΑ***

Information Asset Risk	**Threat**	**Πεδίο Προσοχής**	***Μη εξουσιοδοτημένη πρόσβαση στα Φυσικά Μέσα***			
		(1) Δράστης: *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	Ο δράστης μπορεί να είναι εσωτερικός ή εξωτερικός			
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	Κάποιος που αποκτά πρόσβαση στους χώρους που φυλάσσονται τα φυσικά μέσα εκμεταλλευόμενος ανεπαρκή προστασία των χώρων ή αμέλεια του χρήστη που τα διαχειρίζεται.			
		(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος			
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη**	**Καταστροφή**		
			Τροποποίηση	**Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Απώλεια Εμπιστευτικότητας			
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**	
		(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
				Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
		Η μη εξουσιοδοτημένη πρόσβαση μπορεί να προκαλέσει απώλεια Εμπιστευτικότητας και Ακεραιότητας των ΙΝΔΑ. Η αποκάλυψη των δεδομένων των ασθενών θα επιφέρει σοβαρά προβλήματα αξιοπιστίας στο νοσοκομείο.		Φήμη και εμπιστοσύνη πελατών (4)	3	12
				Οικονομικά (2)	3	6
				Παραγωγικότητα (3)	3	9
				Ασφάλεια και Υγεία (5)	-	-
				Πρόστιμα και Νομικές Κυρώσεις (1)	3	3
					Relative Risk Score	**30**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Φάκελοι Ασθενών	Φύλαξη σε ασφαλή χώρο Ασφαλής διαχείριση από τους χρήστες
Αντίγραφα δεδομένων	Φύλαξη σε ασφαλή χώρο

		Allegro Worksheet 10	***Κίνδυνος για το IT Αγαθο***
		IT Αγαθό	***Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή - ΙΝΔΑ***
Information Asset Risk	**Threat**	**Πεδίο Προσοχής**	***Ακούσιο Λάθος Εξουσιοδοτημένου Χρήστη***
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	1. Λάθος εσωτερικού χρήστη

		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*			
		(3) Κίνητρο: *Γιατί το κάνει;*	Ακούσια		
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Ακεραιότητα του αγαθού		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
			Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
	Η λανθασμένη εισαγωγή δεδομένων θα προκαλέσει απώλεια της Ακεραιότητας των ΙΝΔΑ. Τα λάθη αυτά δεν επιφέρουν σοβαρά προβλήματα αν δεν γίνουν αντιληπτά στις διαδικασίες θεραπευτικής φροντίδας των ασθενών.		Φήμη και εμπιστοσύνη πελατών (4)	2	8
			Οικονομικά (2)	1	2
			Παραγωγικότητα (3)	1	3
			Ασφάλεια και Υγεία (5)	1	5
			Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
				Relative Risk Score	**19**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εφαρμογή	Η εφαρμογή θα έχει διαδικασίες ελέγχου εισαγωγής δεδομένων Η εφαρμογή θα έχει διαδικασίες ελέγχου διπλοεγγραφών

		Allegro Worksheet 10	***Κίνδυνος για το IT Αγαθο***	
		IT Αγαθό	***Ιατρικά/Νοσηλευτικά Δεδομένα Ασθενή - ΙΝΔΑ***	
Information Asset Risk	**Threat**	**Πεδίο Προσοχής**	***Σκόπιμη Βλάβη στο Υλικό***	
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	Υπάλληλος του νοσοκομείου ή τρίτος	
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	Πρέπει να αποκτήσει πρόσβαση στους χώρους του νοσοκομείου όπου υπάρχει εξοπλισμός του ΠΣ.	
		(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος	
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**	

		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*			**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*	
				Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
	Η απώλεια Διαθεσιμότητας των ΙΝΔΑ επιφέρει σοβαρά προβλήματα δυσλειτουργίας στο νοσοκομείο, αφού είναι απαραίτητα για τη διαχείριση του διαδικασιών θεραπευτικής φροντίδας του ασθενή. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα..			Φήμη και εμπιστοσύνη πελατών (4)	3	12
				Οικονομικά (2)	1	2
				Παραγωγικότητα (3)	3	9
				Ασφάλεια και Υγεία (5)	1	5
				Πρόστιμα και Νομικές Κυρώσεις (1)	2	2
					Relative Risk Score	**30**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Δωμάτιο εξυπηρετητών	Έλεγχος φυσικής πρόσβασης Συμβόλαιο Συντήρησης
Δίκτυο Νοσοκομείου	Έλεγχος φυσικής πρόσβασης Συμβόλαιο Συντήρησης
Σταθμοί Εργασίας	Έλεγχος φυσικής πρόσβασης Συμβόλαιο συντήρησης

Allegro Worksheet 8	ΠΡΟΦΙΛ ΚΡΙΣΙΜΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ (IT) A	
(1) Κρίσιμο Αγαθό: *Ποιο είναι το κρίσιμο IT αγαθό;*	**(2) Αιτιολόγηση της Επιλογής:** *Γιατί το IT αγαθό είναι σημαντικό για τον οργανισμό;*	**(3) Περιγραφή:** *Ποια είναι η συμφωνημένη περιγραφή του IT αγαθού;*
Δεδομένα Ραντεβού Ασθενή - ΔΡΑ	Α. Είναι απαραίτητα για την εύρυθμη λειτουργία των ΕΙ και ΑΙ και κυρίως για την άρτια εξυπηρέτηση των εξωτερικών ασθενών.	ΔΡΑ: Πρόγραμμα ΕΙ και ΑΙ, Ραντεβού Ασθενών Το αγαθό χρειάζεται στις διαδικασίες των: - Γραμματεία Ε.Ι. – Α.Ι.
(4) Ιδιοκτήτης/τες: *Σε ποιους ανήκει το IT αγαθό;*		
- Πάροχος Υποσυστήματος Ραντεβού Ασθενή		
(5) Απαιτήσεις Ασφάλειας: *Ποιες είναι οι απαιτήσεις ασφάλειας για το IT αγαθό;*		
Εμπιστευτικότητα **(Confidentiality)**	Μόνο εξουσιοδοτημένο προσωπικό του νοσοκομείου μπορεί να δει το αγαθό ως εξής:	Τα ΔΡΑ μπορεί να δει το προσωπικό των τμημάτων: - Πάροχος Υποσυστήματος Ραντεβού Ασθενή - Γραμματεία Ε.Ι. – Α.Ι.
	Μόνο εξουσιοδοτημένο προσωπικό των παρόχων μπορεί να δει το αγαθό ως εξής:	Τα ΔΧΑ μπορεί να δει το προσωπικό των παρόχων: - Πάροχος Υποσυστήματος Ραντεβού Ασθενή
Ακεραιότητα **(Integrity)**	Μόνο εξουσιοδοτημένο προσωπικό του νοσοκομείου μπορεί να τροποποιήσει το αγαθό ως εξής:	Η διαχείριση των ΔΡΑ (Εισαγωγή, Διαγραφή, Τροποποίηση) μπορεί να γίνει από το εξουσιοδοτημένο προσωπικό των τμημάτων: - Πάροχος Υποσυστήματος Ραντεβού Ασθενή - Γραμματεία Ε.Ι. – Α.Ι.
	Μόνο εξουσιοδοτημένο προσωπικό του παρόχου μπορεί να τροποποιήσει το αγαθό ως εξής:	Η διαχείριση των ΔΡΑ (Εισαγωγή, Διαγραφή, Τροποποίηση) μπορεί να γίνει από εξουσιοδοτημένο προσωπικό των παρόχων: - Πάροχος Υποσυστήματος Ραντεβού Ασθενή
Διαθεσιμότητα **(Availability)**	Το εξουσιοδοτημένο προσωπικό πρέπει να έχει πρόσβαση το αγαθό ως εξής:	Τα ΔΡΑ πρέπει να είναι διαθέσιμα στα παρακάτω τμήματα για τις ημέρες λειτουργίας τους: - Γραμματεία Ε.Ι. – Α.Ι.
	Το αγαθό πρέπει να είναι διαθέσιμο για **24** ώρες, **7** μέρες/εβδομάδα, **52** εβδομάδες/χρόνο.	Το ΔΧΑ πρέπει να είναι διαθέσιμο κατά τη διάρκεια λειτουργίας των τμημάτων που το χρησιμοποιούν.
Άλλο	Το αγαθό υπόκειται σε νόμους για την ασφάλεια ως εξής:	Τα ραντεβού των ασθενών είναι εμπιστευτική πληροφορία.
(6) Σημαντικότερες Απαιτήσεις Ασφάλειας: *Ποιες είναι οι σημαντικότερες απαιτήσεις ασφάλειας για το IT αγαθό;*		

Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα	Άλλο

Allegro Worksheet 9a	ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (ΤΕΧΝΙΚΟ)
ΕΣΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**
Σταθμοί Εργασίας ΕΙ - ΑΙ	Γραμματεία ΕΙ - ΑΙ
Δίκτυο του Νοσοκομείου, μέσω του οποίου μεταδίδονται τα δεδομένα.	Τ.Π.Ο.

ΕΞΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**
Internet. Διαδικτυακή διαχείριση της εφαρμογής	

Allegro Worksheet 9b	ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (ΦΥΣΙΚΟ)
ΕΣΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**
Χειρόγραφος Φάκελος Ασθενή	Γραμματεία ΕΙ - ΑΙ
ΕΞΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**
Οι Περιέκτες του Παρόχου	Πάροχος Υποσυστήματος Ραντεβού Ασθενή

Allegro Worksheet 9c	ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (ΑΝΘΡΩΠΟΙ)
ΕΣΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΟΝΟΜΑ Ή ΡΟΛΟΣ/ΑΡΜΟΔΙΟΤΗΤΑ	**ΤΜΗΜΑ/ΜΟΝΑΔΑ**
Προσωπικό Γραμματείας Ε.Ι. – Α.Ι.	Γραμματεία Ε.Ι. – Α.Ι.
ΕΞΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΑΝΑΔΟΧΟΣ, ΠΡΟΜΗΘΕΥΤΗΣ, ΚΛΠ.	**ΟΡΓΑΝΙΣΜΟΣ**
Προσωπικό Παρόχου Υποσυστήματος Ραντεβού Ασθενή	Πάροχος Υποσυστήματος Ραντεβού Ασθενή

Allegro Worksheet 10		ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ			
Information Asset Risk	Threat	**IT Αγαθό**	***Δεδομένα Ραντεβού Ασθενή - ΔΡΑ***		
		Πεδίο Προσοχής	***Αστοχία Δικτύου***		
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*			
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*			
		(3) Κίνητρο: *Γιατί το κάνει;*			
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
			Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
	Η απώλεια Διαθεσιμότητας των ΔΡΑ δεν θα επιφέρει σοβαρά προβλήματα. Μπορεί να επιφέρει καθυστερήσεις της λειτουργίας		Φήμη και εμπιστοσύνη πελατών (4)	2	8

	στο νοσοκομείο.	Οικονομικά (2)	-	-
		Παραγωγικότητα (3)	1	3
		Ασφάλεια και Υγεία (5)	-	-
		Πρόστιμα και Νομικές Κυρώσεις (1)	-	-
			Relative Risk Score	**11**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Δίκτυο Νοσοκομείου	Έλεγχοι προστασίας από φυσικές καταστροφές Έλεγχοι προστασίας από διακοπή ηλεκτροδότησης Συμβόλαιο Συντήρησης
Εξωτερικός Συνεργάτης	Συμβόλαιο συντήρησης και υποχρεώσεις για την ασφάλεια των ΔΡΑ

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**		
Information Asset Risk	**Threat**	**IT Αγαθό**	***Δεδομένα Ραντεβού Ασθενή - ΔΡΑ***	
		Πεδίο Προσοχής	***Μη εξουσιοδοτημένη χρήση εφαρμογής***	
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	1. Εσωτερικός χρήστης που έχει υποκλέψει συνθηματικά 2. Εξωτερικός χρήστης που έχει αποκτήσει πρόσβαση μέσω του δικτύου και έχει ανακαλύψει συνθηματικά	
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	1. Ο εσωτερικός χρήστης εκμεταλλευόμενος αμέλεια στη φύλαξη των συνθηματικών ενός νόμιμου χρήστη 2. Ο εξωτερικός χρήστης εκμεταλλευόμενος αδυναμία στην ασφάλεια του δικτύου	
		(3) Κίνητρο: *Γιατί το κάνει;*		
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**	
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Απώλεια Ακεραιότητας	
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια** **Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*	
			Πεδίο Επιπτώσεων	**Αξία** **Βαθμός**
	Η απώλεια Διαθεσιμότητας των ΔΡΑ δεν θα επιφέρει σοβαρά προβλήματα. Μπορεί να επιφέρει καθυστερήσεις της λειτουργίας		Φήμη και εμπιστοσύνη πελατών (4)	2 8

	στο νοσοκομείο.	Οικονομικά (2)	-	-
		Παραγωγικότητα (3)	1	3
		Ασφάλεια και Υγεία (5)	-	-
		Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
			Relative Risk Score	**12**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εφαρμογή ΔΡΑ	Έλεγχοι πρόσβασης στις εφαρμογές
Εξωτερικός Συνεργάτης	Συμβόλαιο συντήρησης και υποχρεώσεις για την ασφάλεια των ΔΡΑ

Allegro Worksheet 8	ΠΡΟΦΙΛ ΚΡΙΣΙΜΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ (IT) A	
(1) Κρίσιμο Αγαθό: *Ποιο είναι το κρίσιμο IT αγαθό;*	**(2) Αιτιολόγηση της Επιλογής:** *Γιατί το IT αγαθό είναι σημαντικό για τον οργανισμό;*	**(3) Περιγραφή:** *Ποια είναι η συμφωνημένη περιγραφή του IT αγαθού;*
Υπηρεσιακά/Μισθολογικά δεδομένα Προσωπικού HOSPITAL – ΥΜΔΠ	Τα ΥΜΔΠ είναι απαραίτητα: Α. Για τη διαχείριση του προσωπικού (Πρόσληψη, Εξέλιξη, άδειες κλπ) Β. Για τη διαχείριση της μισθοδοσίας του προσωπικού	ΥΜΔΠ: Δεδομένα πρόσληψης, βαθμολογικών κατατάξεων, προσόντων, ποινές, υπερωρίες, μισθολογικά δεδομένα. Στοιχεία των ΥΜΔΠ εκτός της ηλεκτρονικής μορφής εκτυπώνονται στα: - Εκκαθαριστικά πληρωμών - Βεβαιώσεις
(4) Ιδιοκτήτης/τες: *Σε ποιους ανήκει το IT αγαθό;*		
- Τμήμα Προσωπικού - Τμήμα Μισθοδοσίας		
(5) Απαιτήσεις Ασφάλειας: *Ποιες είναι οι απαιτήσεις ασφάλειας για το IT αγαθό;*		
Εμπιστευτικότητα (Confidentiality)	Μόνο εξουσιοδοτημένο προσωπικό του νοσοκομείου μπορεί να δει το αγαθό ως εξής:	Τα ΥΜΔΠ μπορεί να δει το προσωπικό των τμημάτων: - Τμήμα Προσωπικού - Τμήμα Μισθοδοσίας - Τ.Π.Ο
	Μόνο εξουσιοδοτημένο προσωπικό των παρόχων μπορεί να δει το αγαθό ως εξής:	Τα ΥΜΔΠ μπορεί να δει το προσωπικό του παρόχου: - Πάροχος Υποσυστήματος Διαχείρισης Προσωπικού/Μισθοδοσία
Ακεραιότητα (Integrity)	Μόνο εξουσιοδοτημένο προσωπικό του νοσοκομείου μπορεί να τροποποιήσει το αγαθό ως εξής:	Η διαχείριση των ΥΜΔΠ (Εισαγωγή, Διαγραφή, Τροποποίηση) μπορεί να γίνει από το εξουσιοδοτημένο προσωπικό των τμημάτων: - Τμήμα Προσωπικού - Τμήμα Μισθοδοσίας
	Μόνο εξουσιοδοτημένο προσωπικό του παρόχου μπορεί να τροποποιήσει το αγαθό ως εξής:	Η διαχείριση των ΥΜΔΠ (Εισαγωγή, Διαγραφή, Τροποποίηση) μπορεί να γίνει από εξουσιοδοτημένο προσωπικό του παρόχου: - Πάροχος Υποσυστήματος Διαχείρισης Προσωπικού/Μισθοδοσίας
Διαθεσιμότητα (Availability)	Το εξουσιοδοτημένο προσωπικό πρέπει να έχει πρόσβαση το αγαθό ως εξής:	Τα ΥΜΔΠ πρέπει να είναι διαθέσιμα στα παρακάτω τμήματα για τις ημέρες λειτουργίας τους: - Τμήμα Προσωπικού - Τμήμα Μισθοδοσίας
	Το αγαθό πρέπει να είναι διαθέσιμο για **24** ώρες, **7** μέρες/εβδομάδα, **52** εβδομάδες/χρόνο.	Τα ΥΜΔΠ πρέπει να είναι διαθέσιμο κατά τη διάρκεια λειτουργίας των τμημάτων που το χρησιμοποιούν.
Άλλο	Το αγαθό υπόκειται σε νόμους για την ασφάλεια ως εξής:	Τα ΥΜΔΠ είναι εμπιστευτικά δεδομένα.
(6) Σημαντικότερες Απαιτήσεις Ασφάλειας: *Ποιες είναι οι σημαντικότερες απαιτήσεις ασφάλειας για το IT αγαθό;*		
Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα	Άλλο

Allegro Worksheet 9a	ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (ΤΕΧΝΙΚΟ)	
ΕΣΩΤΕΡΙΚΟ		
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ		ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)
Υποσύστημα Διαχείρισης Προσωπικού/Μισθοδοσίας. Βρίσκεται στο Διοικητικό – Οικονομικό Υποσύστημα που αποτελείται από: α) Συστοιχία (cluster) δύο servers β) Βάση δεδομένων Microsoft SQL 2000 γ) Εφαρμογή Διαχείρισης Ασθενή.		Υ.Π.Ε. Τ.Π.Ο.
Δίκτυο του Νοσοκομείου, μέσω του οποίου μεταδίδονται τα δεδομένα.		Τ.Π.Ο.
Σταθμοί Εργασίας του Νοσοκομείου.		Τ.Π.Ο. Χρήστης Σταθμού Εργασίας
ΕΞΩΤΕΡΙΚΟ		
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ		ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)
Internet. Αποστολή μέσω διαδικτύου μισθοδοσίας σε Τράπεζα.		

Allegro Worksheet 9b	ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (ΦΥΣΙΚΟ)	
ΕΣΩΤΕΡΙΚΟ		
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ		ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)
Χειρόγραφος Φάκελος Υπαλλήλου		Τμ. Προσωπικού
Βεβαιώσεις, καρτέλα αδειών, διοικητικές αποφάσεις, εκκαθαριστικά.		Τμ. Προσωπικού Μισθοδοσία Προσωπικό
ΕΞΩΤΕΡΙΚΟ		
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ		ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)
Αντίγραφα σε χαρτί μέρους των πληροφοριών δίνονται σε Τράπεζες		Τράπεζες
Αντίγραφα σε χαρτί των πληροφοριών δίνονται στα Ασφαλιστικά ταμεία		Ασφαλιστικά Ταμεία

Allegro Worksheet 9c	ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (ΑΝΘΡΩΠΟΙ)	
ΕΣΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ		
ΟΝΟΜΑ Ή ΡΟΛΟΣ/ΑΡΜΟΔΙΟΤΗΤΑ		ΤΜΗΜΑ/ΜΟΝΑΔΑ
Προσωπικό Τμήματος Προσωπικού		Τμήμα Προσωπικού
Προσωπικό Τμήματος Μισθοδοσίας		Τμήμα Μισθοδοσίας
ΕΞΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ		
ΑΝΑΔΟΧΟΣ, ΠΡΟΜΗΘΕΥΤΗΣ, ΚΛΠ.		ΟΡΓΑΝΙΣΜΟΣ
Προσωπικό Παρόχου Υποσυστήματος Διαχείρισης Προσωπικού/Μισθοδοσίας		Πάροχος Υποσυστήματος Διοικητικού – Οικονομικού Υποσυστήματος
Προσωπικό Τραπεζών		Τράπεζες
Προσωπικό Ασφαλιστικών Ταμείων		Ασφαλιστικά Ταμεία

Allegro Worksheet 10		ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ			
Information Asset Risk	IT Αγαθό		Υπηρεσιακά/Μισθολογικά δεδομένα Προσωπικού HOSPITAL – ΥΜΔΠ		
		Πεδίο Προσοχής	***Αστοχία Υλικού***		
	Threat	**(1) Δράστης :** *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*			
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*			
		(3) Κίνητρο: *Γιατί το κάνει;*			
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η απώλεια Διαθεσιμότητας των ΥΜΔΠ επιφέρει σοβαρά προβλήματα στη διαχείριση της μισθοδοσίας και του προσωπικού. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα.	Φήμη και εμπιστοσύνη πελατών (4)	3	12
	Οικονομικά (2)	1	2
	Παραγωγικότητα (3)	2	6
	Ασφάλεια και Υγεία (5)	-	-
	Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
	Relative Risk Score		**21**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εξυπηρετητές	Συμβόλαιο συντήρησης Σχέδιο Ανάκαμψης από Καταστροφής
Βάση δεδομένων	Συμβόλαιο συντήρησης Αντίγραφα Ασφάλειας
Δίκτυο Νοσοκομείου	Συμβόλαιο Συντήρησης

Allegro Worksheet 10		ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ			
Information Asset Risk	Threat	IT Αγαθό	Υπηρεσιακά/Μισθολογικά δεδομένα Προσωπικού HOSPITAL – ΥΜΔΠ		
		Πεδίο Προσοχής	***Αστοχία Λογισμικού***		
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*			
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*			
		(3) Κίνητρο: *Γιατί το κάνει;*			
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η απώλεια Διαθεσιμότητας των ΥΜΔΠ επιφέρει σοβαρά προβλήματα στη διαχείριση της μισθοδοσίας και του προσωπικού. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα.	Φήμη και εμπιστοσύνη πελατών (4)	2	6
	Οικονομικά (2)	-	-
	Παραγωγικότητα (3)	2	6
	Ασφάλεια και Υγεία (5)	-	-
	Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
	Relative Risk Score		**13**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Λογισμικό Εφαρμογών – Εξυπηρετητών – Βάσεις δεδομένων	Έλεγχος αλλαγών Συμβόλαιο συντήρησης Αντίγραφα Ασφάλειας

Allegro Worksheet 10		ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ	
Information Asset Risk	Threat	IT Αγαθό	Υπηρεσιακά/Μισθολογικά δεδομένα Προσωπικού HOSPITAL – ΥΜΔΠ
		Πεδίο Προσοχής	***Φυσική Καταστροφή***

		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*			
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*			
		(3) Κίνητρο: *Γιατί το κάνει;*			
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η απώλεια Διαθεσιμότητας των ΥΜΔΠ επιφέρει σοβαρά προβλήματα στη διαχείριση της μισθοδοσίας και του προσωπικού. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα.	Φήμη και εμπιστοσύνη πελατών (4)	3	12
	Οικονομικά (2)	1	2
	Παραγωγικότητα (3)	2	6
	Ασφάλεια και Υγεία (5)	-	-
	Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
		Relative Risk Score	**21**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Δωμάτιο εξυπηρετητών	Έλεγχοι προστασίας από φυσικές καταστροφές
Εξυπηρετητές	Συμβόλαιο συντήρησης Σχέδιο Ανάκαμψης από Καταστροφής
Δίκτυο Νοσοκομείου	Έλεγχοι προστασίας από φυσικές καταστροφές Συμβόλαιο Συντήρησης

		Allegro Worksheet 10	***Κίνδυνος για το IT Αγαθο***	
		IT Αγαθό	**Υπηρεσιακά/Μισθολογικά δεδομένα Προσωπικού HOSPITAL – ΥΜΔΠ**	
Information Asset Risk	**Threat**	**Πεδίο Προσοχής**	***Σκόπιμη Βλάβη στο Υλικό***	
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	Υπάλληλος του νοσοκομείου ή τρίτος	

		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	Πρέπει να αποκτήσει πρόσβαση στους χώρους του νοσοκομείου όπου υπάρχει εξοπλισμός του ΠΣ.		
		(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος		
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
		Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η απώλεια Διαθεσιμότητας των ΥΜΔΠ επιφέρει σοβαρά προβλήματα στη διαχείριση της μισθοδοσίας και του προσωπικού. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα.		Φήμη και εμπιστοσύνη πελατών (4)	3	12
		Οικονομικά (2)	1	2
		Παραγωγικότητα (3)	2	6
		Ασφάλεια και Υγεία (5)	-	-
		Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
			Relative Risk Score	**21**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Δωμάτιο εξυπηρετητών	Έλεγχος φυσικής πρόσβασης Συμβόλαιο Συντήρησης
Δίκτυο Νοσοκομείου	Έλεγχος φυσικής πρόσβασης Συμβόλαιο Συντήρησης
Σταθμοί Εργασίας	Έλεγχος φυσικής πρόσβασης Συμβόλαιο συντήρησης

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**	
Information Asset Risk	**Threat**	**IT Αγαθό**	**Υπηρεσιακά/Μισθολογικά δεδομένα Προσωπικού HOSPITAL – ΥΜΔΠ**
		Πεδίο Προσοχής	***Μη εξουσιοδοτημένη πρόσβαση στο Υποσύστημα Προσωπικού***
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	1. Εσωτερικός χρήστης που έχει υποκλέψει συνθηματικά 2. Εξωτερικός χρήστης που έχει αποκτήσει πρόσβαση μέσω του δικτύου και έχει ανακαλύψει συνθηματικά

		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	1. Ο εσωτερικός χρήστης εκμεταλλευόμενος αμέλεια στη φύλαξη των συνθηματικών ενός νόμιμου χρήστη 2. Ο εξωτερικός χρήστης εκμεταλλευόμενος αδυναμία στην ασφάλεια του δικτύου		
		(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος		
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Απώλεια Εμπιστευτικότητας και Ακεραιότητας		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η μη εξουσιοδοτημένη πρόσβαση μπορεί να προκαλέσει απώλεια Εμπιστευτικότητας και Ακεραιότητας των ΥΜΔΠ. Στα δεδομένα αυτά εμπεριέχονται ευαίσθητα προσωπικά δεδομένα.	Φήμη και εμπιστοσύνη πελατών (4)	2	8
	Οικονομικά (2)	2	4
	Παραγωγικότητα (3)	2	6
	Ασφάλεια και Υγεία (5)	-	-
	Πρόστιμα και Νομικές Κυρώσεις (1)	3	3
		Relative Risk Score	**21**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αποδοχή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εξυπηρετητές	Έλεγχος πρόσβασης Παρακολούθηση τρίτων που έχουν πρόσβαση
Βάση δεδομένων	Πρόσβαση μόνο μέσω της εφαρμογής Παρακολούθηση τρίτων που έχουν πρόσβαση Αντίγραφα Ασφάλειας
Δίκτυο Νοσοκομείου, ΚΥ	Έλεγχοι διείσδυσης (penetration testing) Εγκατάσταση αναχωμάτων ασφάλειας (firewalls)
Σταθμοί Εργασίας	Αυθεντικοποίηση χρηστών στο λειτουργικό και στις εφαρμογές Ενεργοποίηση οθόνης αδράνειας

Allegro Worksheet 10			ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ			
Information Asset Risk		IT Αγαθό	**Υπηρεσιακά/Μισθολογικά δεδομένα Προσωπικού HOSPITAL – ΥΜΔΠ**			
		Πεδίο Προσοχής	***Μη εξουσιοδοτημένη πρόσβαση στα Φυσικά Μέσα***			
	Threat	**(1) Δράστης :** *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	Ο δράστης μπορεί να είναι εσωτερικός ή εξωτερικός			
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	Κάποιος που αποκτά πρόσβαση στους χώρους που φυλάσσονται τα φυσικά μέσα εκμεταλλευόμενος ανεπαρκή προστασία των χώρων ή αμέλεια του χρήστη που τα διαχειρίζεται.			
		(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος			
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη**	**Καταστροφή**		
			Τροποποίηση	**Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Απώλεια Εμπιστευτικότητας			
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**	
		(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
				Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
		Η μη εξουσιοδοτημένη πρόσβαση μπορεί να προκαλέσει απώλεια Εμπιστευτικότητας. Τα δεδομένα των υπαλλήλων είναι εμπιστευτικά δεδομένα.		Φήμη και εμπιστοσύνη πελατών (4)	2	8
				Οικονομικά (2)	2	4
				Παραγωγικότητα (3)	2	6
				Ασφάλεια και Υγεία (5)	-	-
				Πρόστιμα και Νομικές Κυρώσεις (1)	3	3
					Relative Risk Score	**21**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αποδοχή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Έγγραφα μισθοδοσίας και προσωπικού	Φύλαξη σε ασφαλή χώρο Οι υπάλληλοι θα παίρνουν τα απαραίτητα μέτρα ασφάλειας των εγγράφων
Αντίγραφα δεδομένων	Φύλαξη σε ασφαλή χώρο

Allegro Worksheet 10	ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ				
Information Asset Risk	IT Αγαθό	Υπηρεσιακά/Μισθολογικά δεδομένα Προσωπικού HOSPITAL – ΥΜΔΠ			
	Πεδίο Προσοχής	***Ακούσιο Λάθος Εξουσιοδοτημένου Χρήστη***			
Threat	**(1) Δράστης :** *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	1. Εσωτερικός χρήστης			
	(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*				
	(3) Κίνητρο: *Γιατί το κάνει;*	Ακούσια			
	(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Τροποποίηση**	**Καταστροφή** **Διακοπή**		
	(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Απώλεια Ακεραιότητας			
	(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**	

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η λανθασμένη εισαγωγή δεδομένων θα προκαλέσει απώλεια της Ακεραιότητας των ΥΜΔΠ. Τα λάθη αυτά δεν επιφέρουν σοβαρά προβλήματα και μπορούν να διορθωθούν όταν ανακαλυφθούν.	Φήμη και εμπιστοσύνη πελατών (4)	2	8
	Οικονομικά (2)	2	4
	Παραγωγικότητα (3)	2	6
	Ασφάλεια και Υγεία (5)	-	-
	Πρόστιμα και Νομικές Κυρώσεις (1)	3	3
	Relative Risk Score		**14**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αποδοχή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εφαρμογή	Η εφαρμογή θα έχει διαδικασίες ελέγχου εισαγωγής δεδομένων Η εφαρμογή θα έχει διαδικασίες ελέγχου διπλοεγγραφών

Allegro Worksheet 8	ΠΡΟΦΙΛ ΚΡΙΣΙΜΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ (IT) A	
(1) Κρίσιμο Αγαθό: *Ποιο είναι το κρίσιμο IT αγαθό;*	**(2) Αιτιολόγηση της Επιλογής:** *Γιατί το IT αγαθό είναι σημαντικό για τον οργανισμό;*	**(3) Περιγραφή:** *Ποια είναι η συμφωνημένη περιγραφή του IT αγαθού;*
Οικονομικά/Λογιστικά Δεδομένα - ΟΛΔ	Τα ΟΛΔ είναι απαραίτητα για τις οικονομικές/λογιστικές διαδικασίες του Hospital	ΟΛΔ: Δεδομένα προϋπολογισμού, εισπρακτέοι και πληρωτέοι λογαριασμοί, Πάγια, Τιμολόγια .
(4) Ιδιοκτήτης/τες: *Σε ποιους ανήκει το IT αγαθό;*		
- Λογιστήριο Hospital		
(5) Απαιτήσεις Ασφάλειας: *Ποιες είναι οι απαιτήσεις ασφάλειας για το IT αγαθό;*		
Εμπιστευτικότητα (Confidentiality)	Μόνο εξουσιοδοτημένο προσωπικό του νοσοκομείου μπορεί να δει το αγαθό ως εξής:	Τα ΟΛΔ μπορεί να δει το προσωπικό των τμημάτων: - Λογιστήριο Ορισμένα στοιχεία των ΟΛΔ μπορεί να δει το προσωπικό των Προμηθειών
	Μόνο εξουσιοδοτημένο προσωπικό των παρόχων μπορεί να δει το αγαθό ως εξής:	Τα ΥΜΔΠ μπορεί να δει το προσωπικό του παρόχου: - Πάροχος Υποσυστήματος Διοικητικού / Οικονομικού
Ακεραιότητα (Integrity)	Μόνο εξουσιοδοτημένο προσωπικό του νοσοκομείου μπορεί να τροποποιήσει το αγαθό ως εξής:	Η διαχείριση των ΟΛΔ πορεί να γίνει από το εξουσιοδοτημένο προσωπικό των τμημάτων: - Λογιστήριο Hospital
	Μόνο εξουσιοδοτημένο προσωπικό του παρόχου μπορεί να τροποποιήσει το αγαθό ως εξής:	Η διαχείριση των ΟΛΔ μπορεί να γίνει από εξουσιοδοτημένο προσωπικό του παρόχου: - Πάροχος Υποσυστήματος Διοικητικού / Οικονομικού
Διαθεσιμότητα (Availability)	Το εξουσιοδοτημένο προσωπικό πρέπει να έχει πρόσβαση το αγαθό ως εξής:	Τα ΟΛΔ πρέπει να είναι διαθέσιμα στα παρακάτω τμήματα για τις ημέρες λειτουργίας τους: - Λογιστήριο Hospital
	Το αγαθό πρέπει να είναι διαθέσιμο για **24** ώρες, **7** μέρες/εβδομάδα, **52** εβδομάδες/χρόνο.	Τα ΟΛΔ πρέπει να είναι διαθέσιμο κατά τη διάρκεια λειτουργίας των τμημάτων που το χρησιμοποιούν.
Άλλο	Το αγαθό υπόκειται σε νόμους για την ασφάλεια ως εξής:	
(6) Σημαντικότερες Απαιτήσεις Ασφάλειας: *Ποιες είναι οι σημαντικότερες απαιτήσεις ασφάλειας για το IT αγαθό;*		
Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα	Άλλο
Allegro Worksheet 9a	ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (ΤΕΧΝΙΚΟ)		
ΕΣΩΤΕΡΙΚΟ			

ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)
Τα ΟΛΔ βρίσκονται στο Υποσύστημα Διοικητικού/Οικονομικού που αποτελείται από: α) Συστοιχία (cluster) δύο servers β) Βάση δεδομένων Microsoft SQL 2000 γ) Εφαρμογή Διοικητικού/Οικονομικού	Υ.Π.Ε.
	Τ.Π.Ο.
Δίκτυο του Νοσοκομείου, μέσω του οποίου μεταδίδονται τα δεδομένα.	Τ.Π.Ο.
Σταθμοί Εργασίας του Νοσοκομείου.	Τ.Π.Ο.
	Χρήστης Σταθμού Εργασίας
ΕΞΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**
Internet. Αποστολή στοιχείων σε προμηθευτές ή σε διοικητικές υπηρεσίες μέσω διαδικτύου.	

Allegro Worksheet 9b	ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (ΦΥΣΙΚΟ)

ΕΣΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**
Έγγραφα λογιστηρίου	Λογιστήριο
ΕΞΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**
Αντίγραφα σε χαρτί μέρους των πληροφοριών δίνονται σε Τράπεζες	Τράπεζες
Αντίγραφα σε χαρτί των πληροφοριών δίνονται στα Ασφαλιστικά ταμεία	Ασφαλιστικά Ταμεία

Allegro Worksheet 9c	ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (ΑΝΘΡΩΠΟΙ)

ΕΣΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΟΝΟΜΑ ΄Η ΡΟΛΟΣ/ΑΡΜΟΔΙΟΤΗΤΑ	**ΤΜΗΜΑ/ΜΟΝΑΔΑ**
Προσωπικό Λογιστηρίου	Λογιστήριο
Προσωπικό Προμηθειών	Προμήθειες
ΕΞΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΑΝΑΔΟΧΟΣ, ΠΡΟΜΗΘΕΥΤΗΣ, ΚΛΠ.	**ΟΡΓΑΝΙΣΜΟΣ**
Προσωπικό Παρόχου Υποσυστήματος Διαχείρισης Διοικητικού/Οικονομικού	Πάροχος Υποσυστήματος Διοικητικού – Οικονομικού Υποσυστήματος

Allegro Worksheet 10		ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ	
Information Asset Risk	Threat	**IT Αγαθό**	**Οικονομικά/Λογιστικά Δεδομένα - ΟΛΔ**
		Πεδίο Προσοχής	***Αστοχία Υλικού***
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	

		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*			
		(3) Κίνητρο: *Γιατί το κάνει;*			
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η απώλεια Διαθεσιμότητας των ΟΛΔ επιφέρει σοβαρά προβλήματα στη διαχείριση του. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα.	Φήμη και εμπιστοσύνη πελατών (4)	1	4
	Οικονομικά (2)	3	6
	Παραγωγικότητα (3)	3	9
	Ασφάλεια και Υγεία (5)	-	-
	Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
		Relative Risk Score	**20**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εξυπηρετητές	Συμβόλαιο συντήρησης Σχέδιο Ανάκαμψης από Καταστροφής
Βάση δεδομένων	Συμβόλαιο συντήρησης Αντίγραφα Ασφάλειας
Δίκτυο Νοσοκομείου	Συμβόλαιο Συντήρησης

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**	
Information Asset Risk	**Threat**	**IT Αγαθό**	**Οικονομικά/Λογιστικά Δεδομένα - ΟΛΔ**
		Πεδίο Προσοχής	***Αστοχία Λογισμικού***
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	
		(3) Κίνητρο: *Γιατί το κάνει;*	

		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
			Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
	Η απώλεια Διαθεσιμότητας των ΟΛΔ επιφέρει σοβαρά προβλήματα στη διαχείριση του. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα.		Φήμη και εμπιστοσύνη πελατών (4)	1	4
			Οικονομικά (2)	1	2
			Παραγωγικότητα (3)	2	6
			Ασφάλεια και Υγεία (5)	-	-
			Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
				Relative Risk Score	**13**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Λογισμικό Εφαρμογών – Εξυπηρετητών – Βάσεις δεδομένων	Έλεγχος αλλαγών Συμβόλαιο συντήρησης Αντίγραφα Ασφάλειας

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**		
Information Asset Risk	**Threat**	**IT Αγαθό**	**Οικονομικά/Λογιστικά Δεδομένα - ΟΛΔ**	
		Πεδίο Προσοχής	***Φυσική Καταστροφή***	
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*		
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*		
		(3) Κίνητρο: *Γιατί το κάνει;*		
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**	
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες	

		του αγαθού;			
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
		Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
	Η απώλεια Διαθεσιμότητας των ΟΛΔ επιφέρει σοβαρά προβλήματα στη διαχείριση του. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα	Φήμη και εμπιστοσύνη πελατών (4)	1	4
		Οικονομικά (2)	3	6
		Παραγωγικότητα (3)	3	9
		Ασφάλεια και Υγεία (5)	-	-
		Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
			Relative Risk Score	**20**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Δωμάτιο εξυπηρετητών	Έλεγχοι προστασίας από φυσικές καταστροφές
Εξυπηρετητές	Συμβόλαιο συντήρησης Σχέδιο Ανάκαμψης από Καταστροφής
Δίκτυο Νοσοκομείου	Έλεγχοι προστασίας από φυσικές καταστροφές Συμβόλαιο Συντήρησης

	Allegro Worksheet 10	***Κίνδυνος για το IT Αγαθο***			
	IT Αγαθό	**Οικονομικά/Λογιστικά Δεδομένα - ΟΛΔ**			
Information Asset Risk	**Threat**	**Πεδίο Προσοχής**	***Σκόπιμη Βλάβη στο Υλικό***		
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	Υπάλληλος του νοσοκομείου ή τρίτος		
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	Πρέπει να αποκτήσει πρόσβαση στους χώρους του νοσοκομείου όπου υπάρχει εξοπλισμός του ΠΣ.		
		(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος		
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

	να συμβεί η απειλή;			
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*	
			Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
	Η απώλεια Διαθεσιμότητας των ΟΛΔ επιφέρει σοβαρά προβλήματα στη διαχείριση του νοσοκομείου. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα.		Φήμη και εμπιστοσύνη πελατών (4)	1	4
			Οικονομικά (2)	3	6
			Παραγωγικότητα (3)	3	9
			Ασφάλεια και Υγεία (5)	-	-
			Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
				Relative Risk Score	**20**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Δωμάτιο εξυπηρετητών	Έλεγχος φυσικής πρόσβασης Συμβόλαιο Συντήρησης
Δίκτυο Νοσοκομείου	Έλεγχος φυσικής πρόσβασης Συμβόλαιο Συντήρησης
Σταθμοί Εργασίας	Έλεγχος φυσικής πρόσβασης Συμβόλαιο συντήρησης

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**	
Information Asset Risk		**IT Αγαθό**	**Οικονομικά/Λογιστικά Δεδομένα - ΟΛΔ**
		Πεδίο Προσοχής	***Μη εξουσιοδοτημένη πρόσβαση στο Υποσύστημα Οικονομικού***
	Threat	**(1) Δράστης :** *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	1. Εσωτερικός χρήστης που έχει υποκλέψει συνθηματικά 2. Εξωτερικός χρήστης που έχει αποκτήσει πρόσβαση μέσω του δικτύου και έχει ανακαλύψει συνθηματικά
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	1. Ο εσωτερικός χρήστης εκμεταλλευόμενος αμέλεια στη φύλαξη των συνθηματικών ενός νόμιμου χρήστη 2. Ο εξωτερικός χρήστης εκμεταλλευόμενος αδυναμία στην ασφάλεια του δικτύου
		(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας*	Επηρεάζονται η Ακεραιότητα και η Διαθεσιμότητα

		του αγαθού;			
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*			**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*	
				Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
	Η μη εξουσιοδοτημένη πρόσβαση μπορεί να προκαλέσει απώλεια Εμπιστευτικότητας και Ακεραιότητας των ΟΛΔ. Στα δεδομένα αυτά δεν εμπεριέχονται ευαίσθητα προσωπικά δεδομένα. Κύριο πρόβλημα είναι η ακεραιότητα.			Φήμη και εμπιστοσύνη πελατών (4)	1	4
				Οικονομικά (2)	2	4
				Παραγωγικότητα (3)	2	6
				Ασφάλεια και Υγεία (5)	-	-
				Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
					Relative Risk Score	**15**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αποδοχή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εξυπηρετητές	Έλεγχος πρόσβασης Παρακολούθηση τρίτων που έχουν πρόσβαση
Βάση δεδομένων	Πρόσβαση μόνο μέσω της εφαρμογής Παρακολούθηση τρίτων που έχουν πρόσβαση Αντίγραφα Ασφάλειας
Δίκτυο Νοσοκομείου, ΚΥ	Έλεγχοι διείσδυσης (penetration testing) Εγκατάσταση αναχωμάτων ασφάλειας (firewalls)
Σταθμοί Εργασίας	Αυθεντικοποίηση χρηστών στο λειτουργικό και στις εφαρμογές Ενεργοποίηση οθόνης αδράνειας

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**	
Information Asset Risk	**Threat**	**IT Αγαθό**	**Οικονομικά/Λογιστικά Δεδομένα - ΟΛΔ**
		Πεδίο Προσοχής	***Μη εξουσιοδοτημένη πρόσβαση στα Φυσικά Μέσα***
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	Ο δράστης μπορεί να είναι εσωτερικός ή εξωτερικός
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	Κάποιος που αποκτά πρόσβαση στους χώρους που φυλάσσονται τα φυσικά μέσα εκμεταλλευόμενος ανεπαρκή προστασία των χώρων ή αμέλεια του χρήστη που τα διαχειρίζεται.
		(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος

		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Τροποποίηση**	**Καταστροφή** **Διακοπή**	
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Απώλεια Εμπιστευτικότητας		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η απώλεια Εμπιστευτικότητας για τα ΟΛΔ δεν είναι σημαντικό πρόβλημα.	Φήμη και εμπιστοσύνη πελατών (4)	1	4
	Οικονομικά (2)	1	2
	Παραγωγικότητα (3)	2	6
	Ασφάλεια και Υγεία (5)	-	-
	Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
	Relative Risk Score		**13**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αποδοχή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Έγγραφα μισθοδοσίας και προσωπικού	Φύλαξη σε ασφαλή χώρο Οι υπάλληλοι θα παίρνουν τα απαραίτητα μέτρα ασφάλειας των εγγράφων
Αντίγραφα δεδομένων	Φύλαξη σε ασφαλή χώρο

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**		
Information Asset Risk	**IT Αγαθό**	**Οικονομικά/Λογιστικά Δεδομένα - ΟΛΔ**		
	Πεδίο Προσοχής	***Ακούσιο Λάθος Εξουσιοδοτημένου Χρήστη***		
Threat	**(1) Δράστης :** *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	1. Εσωτερικός χρήστης		
	(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*			
	(3) Κίνητρο: *Γιατί το κάνει;*	Ακούσια		
	(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Τροποποίηση**	**Καταστροφή** **Διακοπή**	

		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό θα τροποποιηθεί.		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η λανθασμένη εισαγωγή δεδομένων θα προκαλέσει απώλεια της Ακεραιότητας των ΟΛΔ. Τα λάθη αυτά επισημαίνονται και μπορούν να διορθωθούν όταν ανακαλυφθούν.	Φήμη και εμπιστοσύνη πελατών (4)	1	4
	Οικονομικά (2)	2	4
	Παραγωγικότητα (3)	2	6
	Ασφάλεια και Υγεία (5)	-	-
	Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
		Relative Risk Score	**15**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αποδοχή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εφαρμογή	Η εφαρμογή θα έχει διαδικασίες ελέγχου εισαγωγής δεδομένων Η εφαρμογή θα έχει διαδικασίες ελέγχου διπλοεγγραφών

Allegro Worksheet 8	ΠΡΟΦΙΛ ΚΡΙΣΙΜΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ (IT) A	
(1) Κρίσιμο Αγαθό: *Ποιο είναι το κρίσιμο IT αγαθό;*	**(2) Αιτιολόγηση της Επιλογής:** *Γιατί το IT αγαθό είναι σημαντικό για τον οργανισμό;*	**(3) Περιγραφή:** *Ποια είναι η συμφωνημένη περιγραφή του IT αγαθού;*
Δεδομένα Προμηθειών - ΔΠ	Τα ΔΠ είναι απαραίτητα για τις διαδικασίες που αφορούν τις προμήθειες του Hospital	ΔΠ: Παραγγελίες Υλικών και Υπηρεσιών, Διαγωνισμοί, Συμβάσεις, Προγραμματισμός Προμηθειών, Απογραφή, Παραλαβή, Διακινήσεις, Διαιτολόγιο για την Αποθήκη Τροφίμων .
(4) Ιδιοκτήτης/τες: *Σε ποιους ανήκει το IT αγαθό;*		
- Αποθήκες - Γρ. Υλικού - Προμήθειες - Λογιστήριο Hospital		
(5) Απαιτήσεις Ασφάλειας: *Ποιες είναι οι απαιτήσεις ασφάλειας για το IT αγαθό;*		
Εμπιστευτικότητα (Confidentiality)	Μόνο εξουσιοδοτημένο προσωπικό του νοσοκομείου μπορεί να δει το αγαθό ως εξής:	Τα ΔΠ μπορεί να δει το προσωπικό των τμημάτων: - Προμήθειες -Γρ. Υλικού - Αποθήκες Ορισμένα στοιχεία των ΔΠ μπορεί να δει το προσωπικό του Λογιστηρίου
	Μόνο εξουσιοδοτημένο προσωπικό των παρόχων μπορεί να δει το αγαθό ως εξής:	Τα ΔΠ μπορεί να δει το προσωπικό του παρόχου: - Πάροχος Υποσυστήματος Διοικητικού / Οικονομικού
Ακεραιότητα (Integrity)	Μόνο εξουσιοδοτημένο προσωπικό του νοσοκομείου μπορεί να τροποποιήσει το αγαθό ως εξής:	Η διαχείριση των ΔΠ πορεί να γίνει από το εξουσιοδοτημένο προσωπικό των τμημάτων: - Αποθήκες - Γρ. Υλικού - Προμήθειες
	Μόνο εξουσιοδοτημένο προσωπικό του παρόχου μπορεί να τροποποιήσει το αγαθό ως εξής:	Η διαχείριση των ΔΠ μπορεί να γίνει από εξουσιοδοτημένο προσωπικό του παρόχου: - Πάροχος Υποσυστήματος Διοικητικού / Οικονομικού
Διαθεσιμότητα (Availability)	Το εξουσιοδοτημένο προσωπικό πρέπει να έχει πρόσβαση το αγαθό ως εξής:	Τα ΔΠ πρέπει να είναι διαθέσιμα στα παρακάτω τμήματα για τις ημέρες λειτουργίας τους: - Αποθήκες - Γρ. Υλικού - Προμήθειες
	Το αγαθό πρέπει να είναι διαθέσιμο για **24** ώρες, **7** μέρες/εβδομάδα, **52** εβδομάδες/χρόνο.	Τα ΔΠ πρέπει να είναι διαθέσιμα κατά τη διάρκεια λειτουργίας των τμημάτων που το χρησιμοποιούν.
Άλλο	Το αγαθό υπόκειται σε νόμους για την ασφάλεια ως εξής:	Τα ΔΠ είναι εμπιστευτικά δεδομένα.
(6) Σημαντικότερες Απαιτήσεις Ασφάλειας: *Ποιες είναι οι σημαντικότερες απαιτήσεις ασφάλειας για το IT αγαθό;*		
Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα	Άλλο

Allegro Worksheet 9a	ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (ΤΕΧΝΙΚΟ)
ΕΣΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**
Τα ΔΠ βρίσκονται στο Υποσύστημα Διοικητικού/Οικονομικού που αποτελείται	Υ.Π.Ε.

από: α) Συστοιχία (cluster) δύο servers β) Βάση δεδομένων Microsoft SQL 2000 γ) Εφαρμογή Διοικητικού/Οικονομικού	Τ.Π.Ο.
Δίκτυο του Νοσοκομείου, μέσω του οποίου μεταδίδονται τα δεδομένα.	Τ.Π.Ο.
Σταθμοί Εργασίας του Νοσοκομείου.	Τ.Π.Ο. Χρήστης Σταθμού Εργασίας
ΕΞΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**
Internet. -Αποστολή στοιχείων σε προμηθευτές ή σε διοικητικές υπηρεσίες μέσω διαδικτύου. -Ανάρτηση στο Διαύγεια	

Allegro Worksheet 9b	**ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ ΙΤ ΑΓΑΘΟΥ (ΦΥΣΙΚΟ)**
ΕΣΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**
1. Τιμολόγια – Δελτία αποστολής, παραγγελίες, αιτήματα από τμήματα 2. Κασέτες αντιγράφων	Προμήθειες Γρ. Υλικού Αποθήκες Λογιστήριο
ΕΞΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**

Allegro Worksheet 9c	**ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ ΙΤ ΑΓΑΘΟΥ (ΑΝΘΡΩΠΟΙ)**
ΕΣΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΟΝΟΜΑ Ή ΡΟΛΟΣ/ΑΡΜΟΔΙΟΤΗΤΑ	**ΤΜΗΜΑ/ΜΟΝΑΔΑ**
Προσωπικό Προμηθειών	Προμήθειες
Προσωπικό Γρ. Υλικού	Γρ. Υλικού
Προσωπικό Αποθηκών	Αποθήκες
Προσωπικό Λογιστηρίου	Λογιστήριο
ΕΞΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΑΝΑΔΟΧΟΣ, ΠΡΟΜΗΘΕΥΤΗΣ, ΚΛΠ.	**ΟΡΓΑΝΙΣΜΟΣ**
Προσωπικό Παρόχου Υποσυστήματος Διαχείρισης Διοικητικού/Οικονομικού	Πάροχος Υποσυστήματος Διοικητικού – Οικονομικού Υποσυστήματος

Allegro Worksheet 10		ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ			
Information Asset Risk	IT Αγαθό	**Δεδομένα Προμηθειών - ΔΠ**			
	Πεδίο Προσοχής	***Αστοχία Υλικού***			
	Threat	**(1) Δράστης :** *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*			
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*			
		(3) Κίνητρο: *Γιατί το κάνει;*			
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η απώλεια Διαθεσιμότητας των ΔΠ επιφέρει σοβαρά προβλήματα στη διαχείριση των προμηθειών του Νοσοκομείου. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα.	Φήμη και εμπιστοσύνη πελατών (4)	2	8
	Οικονομικά (2)	2	4
	Παραγωγικότητα (3)	3	9
	Ασφάλεια και Υγεία (5)	-	-
	Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
	Relative Risk Score		**22**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εξυπηρετητές	Συμβόλαιο συντήρησης Σχέδιο Ανάκαμψης από Καταστροφής
Βάση δεδομένων	Συμβόλαιο συντήρησης Αντίγραφα Ασφάλειας
Δίκτυο Νοσοκομείου	Συμβόλαιο Συντήρησης

Allegro Worksheet 10		ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ			
Information Asset Risk	Threat	**IT Αγαθό**	**Δεδομένα Προμηθειών - ΔΠ**		
		Πεδίο Προσοχής	***Αστοχία Λογισμικού***		
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*			
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*			
		(3) Κίνητρο: *Γιατί το κάνει;*			
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η προσωρινή απώλεια Διαθεσιμότητας των ΔΠ δεν επιφέρει σοβαρά προβλήματα στη διαχείριση.	Φήμη και εμπιστοσύνη πελατών (4)	1	4
	Οικονομικά (2)	1	2
	Παραγωγικότητα (3)	2	6
	Ασφάλεια και Υγεία (5)	-	-
	Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
	Relative Risk Score		**12**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Λογισμικό Εφαρμογών – Εξυπηρετητών – Βάσεις δεδομένων	Έλεγχος αλλαγών Συμβόλαιο συντήρησης Αντίγραφα Ασφάλειας

Allegro Worksheet 10		ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ	
Information Asset Risk	Threat	**IT Αγαθό**	**Δεδομένα Προμηθειών - ΔΠ**
		Πεδίο Προσοχής	***Φυσική Καταστροφή***
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	

		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*			
		(3) Κίνητρο: *Γιατί το κάνει;*			
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η απώλεια Διαθεσιμότητας των ΔΠ επιφέρει σοβαρά προβλήματα στη διαχείριση των προμηθειών του Νοσοκομείου. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα.	Φήμη και εμπιστοσύνη πελατών (4)	2	8
	Οικονομικά (2)	2	4
	Παραγωγικότητα (3)	3	9
	Ασφάλεια και Υγεία (5)	-	-
	Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
		Relative Risk Score	**22**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Δωμάτιο εξυπηρετητών	Έλεγχοι προστασίας από φυσικές καταστροφές
Εξυπηρετητές	Συμβόλαιο συντήρησης Σχέδιο Ανάκαμψης από Καταστροφής
Δίκτυο Νοσοκομείου	Έλεγχοι προστασίας από φυσικές καταστροφές Συμβόλαιο Συντήρησης

		Allegro Worksheet 10	***Κίνδυνος για το IT Αγαθο***
		IT Αγαθό	**<u>Δεδομένα Προμηθειών - ΔΠ</u>**
Information Asset Risk	**Threat**	**Πεδίο Προσοχής**	***<u>Σκόπιμη Βλάβη στο Υλικό</u>***
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	Υπάλληλος του νοσοκομείου ή τρίτος
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	Πρέπει να αποκτήσει πρόσβαση στους χώρους του νοσοκομείου όπου υπάρχει εξοπλισμός του ΠΣ.
		(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος

		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
			Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
	Η απώλεια Διαθεσιμότητας των ΟΛΔ επιφέρει σοβαρά προβλήματα στη διαχείριση του. Σε περίπτωση διακοπής ή καταστροφής τους πρέπει οι υπάλληλοι να δουλέψουν χειρόγραφα έως ότου διορθωθεί το πρόβλημα.		Φήμη και εμπιστοσύνη πελατών (4)	1	4
			Οικονομικά (2)	3	6
			Παραγωγικότητα (3)	3	9
			Ασφάλεια και Υγεία (5)	-	-
			Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
				Relative Risk Score	**20**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Δωμάτιο εξυπηρετητών	Έλεγχος φυσικής πρόσβασης Συμβόλαιο Συντήρησης
Δίκτυο Νοσοκομείου	Έλεγχος φυσικής πρόσβασης Συμβόλαιο Συντήρησης
Σταθμοί Εργασίας	Έλεγχος φυσικής πρόσβασης Συμβόλαιο συντήρησης

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**	
Information Asset Risk	**Threat**	**IT Αγαθό**	**Δεδομένα Προμηθειών - ΔΠ**
		Πεδίο Προσοχής	***Μη εξουσιοδοτημένη πρόσβαση στο Υποσύστημα Οικονομικού***
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	1. Εσωτερικός χρήστης που έχει υποκλέψει συνθηματικά 2. Εξωτερικός χρήστης που έχει αποκτήσει πρόσβαση μέσω του δικτύου και έχει ανακαλύψει συνθηματικά
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	1. Ο εσωτερικός χρήστης εκμεταλλευόμενος αμέλεια στη φύλαξη των συνθηματικών ενός νόμιμου χρήστη 2. Ο εξωτερικός χρήστης εκμεταλλευόμενος αδυναμία στην ασφάλεια του δικτύου
		(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος

		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Επηρεάζεται η Ακεραιότητα και Διαθεσιμότητα		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
			Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
	Η μη εξουσιοδοτημένη πρόσβαση μπορεί να προκαλέσει απώλεια Εμπιστευτικότητας και Ακεραιότητας των ΔΠ. Στα δεδομένα αυτά δεν εμπεριέχονται ευαίσθητα προσωπικά δεδομένα. Κύριο πρόβλημα είναι η ακεραιότητα.		Φήμη και εμπιστοσύνη πελατών (4)	1	4
			Οικονομικά (2)	1	3
			Παραγωγικότητα (3)	2	6
			Ασφάλεια και Υγεία (5)	-	-
			Πρόστιμα και Νομικές Κυρώσεις (1)	-	-
				Relative Risk Score	**13**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αποδοχή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εξυπηρετητές	Έλεγχος πρόσβασης Παρακολούθηση τρίτων που έχουν πρόσβαση
Βάση δεδομένων	Πρόσβαση μόνο μέσω της εφαρμογής Παρακολούθηση τρίτων που έχουν πρόσβαση Αντίγραφα Ασφάλειας
Δίκτυο Νοσοκομείου, ΚΥ	Έλεγχοι διείσδυσης (penetration testing) Εγκατάσταση αναχωμάτων ασφάλειας (firewalls)
Σταθμοί Εργασίας	Αυθεντικοποίηση χρηστών στο λειτουργικό και στις εφαρμογές Ενεργοποίηση οθόνης αδράνειας

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ ΙΤ ΑΓΑΘΟ**	
Information Asset Risk	**Threat**	**IT Αγαθό**	**Δεδομένα Προμηθειών - ΔΠ**
		Πεδίο Προσοχής	***Μη εξουσιοδοτημένη πρόσβαση στα Φυσικά Μέσα***
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	Ο δράστης μπορεί να είναι εσωτερικός ή εξωτερικός
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	Κάποιος που αποκτά πρόσβαση στους χώρους που φυλάσσονται τα φυσικά μέσα εκμεταλλευόμενος ανεπαρκή προστασία των χώρων ή αμέλεια του χρήστη που τα διαχειρίζεται.

		(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος		
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Τροποποίηση**	**Καταστροφή** **Διακοπή**	
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Απώλεια Εμπιστευτικότητας		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η απώλεια Εμπιστευτικότητας για τα ΔΠ δεν είναι σημαντικό πρόβλημα.	Φήμη και εμπιστοσύνη πελατών (4)	1	4
	Οικονομικά (2)	1	2
	Παραγωγικότητα (3)	2	6
	Ασφάλεια και Υγεία (5)	-	-
	Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
	Relative Risk Score		**13**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αποδοχή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Έγγραφα μισθοδοσίας και προσωπικού	Φύλαξη σε ασφαλή χώρο Οι υπάλληλοι θα παίρνουν τα απαραίτητα μέτρα ασφάλειας των εγγράφων
Αντίγραφα δεδομένων	Φύλαξη σε ασφαλή χώρο

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**	
Information Asset Risk		**IT Αγαθό**	**Δεδομένα Προμηθειών - ΔΠ**
		Πεδίο Προσοχής	***Ακούσιο Λάθος Εξουσιοδοτημένου Χρήστη***
	Threat	**(1) Δράστης :** *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	1. Εσωτερικός χρήστης
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	
		(3) Κίνητρο: *Γιατί το κάνει;*	Ακούσια

		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Τροποποίηση**	**Καταστροφή** **Διακοπή**	
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό τροποποιείται λανθασμένα		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η λανθασμένη εισαγωγή δεδομένων θα προκαλέσει απώλεια της Ακεραιότητας των Δπ. Τα λάθη αυτά επισημαίνονται και μπορούν να διορθωθούν όταν ανακαλυφθούν.	Φήμη και εμπιστοσύνη πελατών (4)	1	4
	Οικονομικά (2)	1	2
	Παραγωγικότητα (3)	2	6
	Ασφάλεια και Υγεία (5)	-	-
	Πρόστιμα και Νομικές Κυρώσεις (1)	1	1
		Relative Risk Score	**13**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αποδοχή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εφαρμογή	Η εφαρμογή θα έχει διαδικασίες ελέγχου εισαγωγής δεδομένων Η εφαρμογή θα έχει διαδικασίες ελέγχου διπλοεγγραφών

Allegro Worksheet 8	ΠΡΟΦΙΛ ΚΡΙΣΙΜΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ (IT) A	
(1) Κρίσιμο Αγαθό: Ποιο είναι το κρίσιμο IT αγαθό;	**(2) Αιτιολόγηση της Επιλογής:** Γιατί το IT αγαθό είναι σημαντικό για τον οργανισμό;	**(3) Περιγραφή:** Ποια είναι η συμφωνημένη περιγραφή του IT αγαθού;
Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολλο - ΔΚΓΠ	Τα ΔΚΓΠ είναι απαραίτητα για την διακίνηση των εγγράφων και της αλληλογραφίας του HOSPITAL.	Πρωτόκολλο
(4) Ιδιοκτήτης/τες: Σε ποιους ανήκει το IT αγαθό;		
- Κεντρική Γραμματεία - Πρωτόκολλο		
(5) Απαιτήσεις Ασφάλειας: Ποιες είναι οι απαιτήσεις ασφάλειας για το IT αγαθό;		
Εμπιστευτικότητα (Confidentiality)	Μόνο εξουσιοδοτημένο προσωπικό του νοσοκομείου μπορεί να δει το αγαθό ως εξής:	Τα ΔΚΓΠ μπορεί να δει το προσωπικό των τμημάτων: Κεντρική Γραμματεία / Πρωτόκολλο
	Μόνο εξουσιοδοτημένο προσωπικό των παρόχων μπορεί να δει το αγαθό ως εξής:	Τα ΔΚΓΠ μπορεί να δει το προσωπικό του παρόχου: - Πάροχος Υποσυστήματος Διοικητικού/Οικονομικού
Ακεραιότητα (Integrity)	Μόνο εξουσιοδοτημένο προσωπικό του νοσοκομείου μπορεί να τροποποιήσει το αγαθό ως εξής:	Η διαχείριση των ΔΚΓΠ μπορεί να γίνει από το εξουσιοδοτημένο προσωπικό της Κεντρικής Γραμματείας - Πρωτόκολλου.
	Μόνο εξουσιοδοτημένο προσωπικό του παρόχου μπορεί να τροποποιήσει το αγαθό ως εξής:	Η διαχείριση των ΔΚΓΠ μπορεί να γίνει από εξουσιοδοτημένο προσωπικό του παρόχου: - Πάροχος Υποσυστήματος Εργαστηρίων
Διαθεσιμότητα (Availability)	Το εξουσιοδοτημένο προσωπικό πρέπει να έχει πρόσβαση το αγαθό ως εξής:	Τα ΔΚΓΠ πρέπει να είναι διαθέσιμα για τις ημέρες λειτουργίας της Κεντρικής Γραμματείας - Πρωτόκολλου.
	Το αγαθό πρέπει να είναι διαθέσιμο για **24** ώρες, **7** μέρες/εβδομάδα, **52** εβδομάδες/χρόνο.	Τα ΔΚΓΠ πρέπει να είναι διαθέσιμα κατά τη διάρκεια λειτουργίας της Κεντρικής Γραμματείας - Πρωτόκολλου, δηλαδή 8 ώρες τις καθημερινές.
Άλλο	Το αγαθό υπόκειται σε νόμους για την ασφάλεια ως εξής:	
(6) Σημαντικότερες Απαιτήσεις Ασφάλειας: Ποιες είναι οι σημαντικότερες απαιτήσεις ασφάλειας για το IT αγαθό;		

Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα	Άλλο

Allegro Worksheet 9a	ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (ΤΕΧΝΙΚΟ)
ΕΣΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**
Τα ΔΚΓΠ βρίσκονται στο Υποσύστημα Διοικητικού / Οικονομικού του ΠΚΔ, που αποτελείται από: α) Συστοιχία (cluster) δύο servers	Υ.Πε.
β) Βάση δεδομένων Microsoft SQL 2000 γ) Εφαρμογή Διοικητικού / Οικονομικού	Τ.Π.Ο.
Δίκτυο του Νοσοκομείου, μέσω του οποίου μεταδίδονται τα δεδομένα.	Τ.Π.Ο.
Σταθμοί Εργασίας του Νοσοκομείου.	Τ.Π.Ο.
	Χρήστης Σταθμού Εργασίας

ΕΞΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**

Allegro Worksheet 9b	ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (ΦΥΣΙΚΟ)

ΕΣΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**
Διαβιβαστικά Έγγραφα, Βεβαιώσεις, Αιτήσεις, Πρωτόκολλο	Κεντρική Γραμματεία - Πρωτόκολλο
Παραγγελία Εξετάσεων, Απαντήσεις	Τμήματα του HOSPITAL

ΕΞΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	**ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)**

Allegro Worksheet 9c	ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (ΑΝΘΡΩΠΟΙ)

ΕΣΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΟΝΟΜΑ Ή ΡΟΛΟΣ/ΑΡΜΟΔΙΟΤΗΤΑ	**ΤΜΗΜΑ/ΜΟΝΑΔΑ**
Προσωπικό του Νοσοκομείου	Κεντρική Γραμματεία - Πρωτόκολλο

ΕΞΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΑΝΑΔΟΧΟΣ, ΠΡΟΜΗΘΕΥΤΗΣ, ΚΛΠ.	**ΟΡΓΑΝΙΣΜΟΣ**
Προσωπικό Παρόχου Υποσυστήματος Διοικητικού / Οικονομικού	Πάροχος Υποσυστήματος Υποσυστήματος Διοικητικού / Οικονομικού

Allegro Worksheet 10		ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ			
Information Asset Risk	Threat	**IT Αγαθό**	**Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολλο - ΔΚΓΠ**		
		Πεδίο Προσοχής	***Αστοχία Υλικού***		
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*			
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*			
		(3) Κίνητρο: *Γιατί το κάνει;*			
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
		Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
	Η απώλεια Διαθεσιμότητας των ΔΚΓΠ δεν επιφέρει σοβαρά προβλήματα στη διαχείριση του νοσοκομείου.	Φήμη και εμπιστοσύνη πελατών (4)	1	4
		Οικονομικά (2)	-	-
		Παραγωγικότητα (3)	2	6
		Ασφάλεια και Υγεία (5)	-	-
		Πρόστιμα και Νομικές Κυρώσεις (1)	-	1
			Relative Risk Score	**10**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εξυπηρετητές	Συμβόλαιο συντήρησης Σχέδιο Ανάκαμψης από Καταστροφής
Βάση δεδομένων	Συμβόλαιο συντήρησης Αντίγραφα Ασφάλειας
Δίκτυο Νοσοκομείου	Συμβόλαιο Συντήρησης

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**			
Information Asset Risk	**Threat**	**IT Αγαθό**	**Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολλο - ΔΚΓΠ**		
		Πεδίο Προσοχής	***Αστοχία Λογισμικού***		
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*			
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*			
		(3) Κίνητρο: *Γιατί το κάνει;*			
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
			Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**

	των ΔΚΓΠ δεν επιφέρει σοβαρά προβλήματα στη διαχείριση του νοσοκομείου..	Φήμη και εμπιστοσύνη πελατών (4)	-	-
		Οικονομικά (2)	-	-
		Παραγωγικότητα (3)	2	6
		Ασφάλεια και Υγεία (5)	-	-
		Πρόστιμα και Νομικές Κυρώσεις (1)	-	-
			Relative Risk Score	**6**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Λογισμικό Εφαρμογών – Εξυπηρετητών – Βάσεις δεδομένων	Έλεγχος αλλαγών Συμβόλαιο συντήρησης Αντίγραφα Ασφάλειας

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**			
Information Asset Risk	**Threat**	**IT Αγαθό**	**Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολλο - ΔΚΓΠ**		
		Πεδίο Προσοχής	***Φυσική Καταστροφή***		
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*			
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*			
		(3) Κίνητρο: *Γιατί το κάνει;*			
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη**	**Καταστροφή**	
			Τροποποίηση	**Διακοπή**	
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*			
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
			Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
	Η μη διαθεσιμότητα των ΔΚΓΠ δεν επιφέρει σοβαρά προβλήματα στη διαχείριση του νοσοκομείου.		Φήμη και εμπιστοσύνη πελατών (4)	1	4
			Οικονομικά (2)	-	-

		Παραγωγικότητα (3)	2	6
		Ασφάλεια και Υγεία (5)	-	-
		Πρόστιμα και Νομικές Κυρώσεις (1)	-	-
			Relative Risk Score	**10**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Δωμάτιο εξυπηρετητών	Έλεγχοι προστασίας από φυσικές καταστροφές
Εξυπηρετητές	Συμβόλαιο συντήρησης Σχέδιο Ανάκαμψης από Καταστροφής
Δίκτυο Νοσοκομείου	Έλεγχοι προστασίας από φυσικές καταστροφές Συμβόλαιο Συντήρησης

Allegro Worksheet 10		***Κίνδυνος για το IT Αγαθο***		
	IT Αγαθό	**<u>Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολλο - ΔΚΓΠ</u>**		
Information Asset Risk	**Threat**	**Πεδίο Προσοχής**	***<u>Σκόπιμη Βλάβη στο Υλικό</u>***	
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	Υπάλληλος του νοσοκομείου ή τρίτος	
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	Πρέπει να αποκτήσει πρόσβαση στους χώρους του νοσοκομείου όπου υπάρχει εξοπλισμός του ΠΣ.	
		(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος	
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**	
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες	
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια** **Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η απώλεια διαθεσιμότητας των ΔΚΓΠ δεν επιφέρει σοβαρά προβλήματα στη διαχείριση του νοσοκομείου.	Φήμη και εμπιστοσύνη πελατών (4)	1	4
	Οικονομικά (2)	-	-
	Παραγωγικότητα (3)	2	6
	Ασφάλεια και Υγεία (5)	-	-

		Πρόστιμα και Νομικές Κυρώσεις (1)	-	-
			Relative Risk Score	**10**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Δωμάτιο εξυπηρετητών	Έλεγχος φυσικής πρόσβασης Συμβόλαιο Συντήρησης
Δίκτυο Νοσοκομείου	Έλεγχος φυσικής πρόσβασης Συμβόλαιο Συντήρησης
Σταθμοί Εργασίας	Έλεγχος φυσικής πρόσβασης Συμβόλαιο συντήρησης

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**		
Information Asset Risk	**IT Αγαθό**	**Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολλο - ΔΚΓΠ**		
	Πεδίο Προσοχής	***Μη εξουσιοδοτημένη πρόσβαση στο Υποσύστημα***		
Threat	**(1) Δράστης :** *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	1. Εσωτερικός χρήστης που έχει υποκλέψει συνθηματικά 2. Εξωτερικός χρήστης που έχει αποκτήσει πρόσβαση μέσω του δικτύου και έχει ανακαλύψει συνθηματικά		
	(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	1. Ο εσωτερικός χρήστης εκμεταλλευόμενος αμέλεια στη φύλαξη των συνθηματικών ενός νόμιμου χρήστη 2. Ο εξωτερικός χρήστης εκμεταλλευόμενος αδυναμία στην ασφάλεια του δικτύου		
	(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος		
	(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
	(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Επηρεάζονται η Ακεραιότητα και η Διαθεσιμότητα		
	(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*	
			Πεδίο Επιπτώσεων	**Αξία** / **Βαθμός**
	Η απώλεια διαθεσιμότητας και ακεραιότητας των ΔΚΓΠ δεν επιφέρει σοβαρά προβλήματα στη διαχείριση του νοσοκομείου.		Φήμη και εμπιστοσύνη πελατών (4)	- /
			Οικονομικά (2)	1 / 2
			Παραγωγικότητα (3)	- / -
			Ασφάλεια και Υγεία (5)	- / -

		Πρόστιμα και Νομικές Κυρώσεις (1)	-	-
			Relative Risk Score	**2**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αποδοχή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εξυπηρετητές	Έλεγχος πρόσβασης Παρακολούθηση τρίτων που έχουν πρόσβαση
Βάση δεδομένων	Πρόσβαση μόνο μέσω της εφαρμογής Παρακολούθηση τρίτων που έχουν πρόσβαση Αντίγραφα Ασφάλειας
Δίκτυο Νοσοκομείου, ΚΥ	Έλεγχοι διείσδυσης (penetration testing) Εγκατάσταση αναχωμάτων ασφάλειας (firewalls)
Σταθμοί Εργασίας	Αυθεντικοποίηση χρηστών στο λειτουργικό και στις εφαρμογές Ενεργοποίηση οθόνης αδράνειας

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**			
Information Asset Risk		**IT Αγαθό**	**Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολλο - ΔΚΓΠ**		
		Πεδίο Προσοχής	***Ακούσιο Λάθος Εξουσιοδοτημένου Χρήστη***		
	Threat	**(1) Δράστης :** *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	1. Εσωτερικός χρήστης		
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*			
		(3) Κίνητρο: *Γιατί το κάνει;*	Ακούσια		
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Τροποποίηση**	**Καταστροφή** **Διακοπή**	
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό θα τροποποιηθεί.		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η απώλεια ακεραιότητας των ΔΚΓΠ δεν επιφέρει σοβαρά προβλήματα στη διαχείριση του νοσοκομείου.μπορούν.	Φήμη και εμπιστοσύνη πελατών (4)	-	-
	Οικονομικά (2)	1	2
	Παραγωγικότητα (3)	-	-

		Ασφάλεια και Υγεία (5)	-	-
		Πρόστιμα και Νομικές Κυρώσεις (1)	-	-
			Relative Risk Score	**2**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αποδοχή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εφαρμογή	Η εφαρμογή θα έχει διαδικασίες ελέγχου εισαγωγής δεδομένων Η εφαρμογή θα έχει διαδικασίες ελέγχου διπλοεγγραφών

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**			
Information Asset Risk	**Threat**	**IT Αγαθό**	**Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολλο - ΔΚΓΠ**		
		Πεδίο Προσοχής	***Μη εξουσιοδοτημένη πρόσβαση στα Φυσικά Μέσα***		
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	Ο δράστης μπορεί να είναι εσωτερικός ή εξωτερικός		
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	Κάποιος που αποκτά πρόσβαση στους χώρους που φυλάσσονται τα φυσικά μέσα εκμεταλλευόμενος ανεπαρκή προστασία των χώρων ή αμέλεια του χρήστη που τα διαχειρίζεται.		
		(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος		
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Τροποποίηση**	**Καταστροφή** **Διακοπή**	
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Απώλεια Εμπιστευτικότητας		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η απώλεια Εμπιστευτικότητας για τα ΔΠ δεν είναι σημαντικό πρόβλημα.	Φήμη και εμπιστοσύνη πελατών (4)	-	-
	Οικονομικά (2)	-	-
	Παραγωγικότητα (3)	-	-
	Ασφάλεια και Υγεία (5)	-	-
	Πρόστιμα και Νομικές Κυρώσεις (1)	-	-
		Relative Risk Score	**13**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	Αποδοχή	Ελαχιστοποίηση	Μεταβίβαση
Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:			
Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*		
Αντίγραφα δεδομένων	Φύλαξη σε ασφαλή χώρο		

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**		
Information Asset Risk	**IT Αγαθό**	**Δεδομένα Κεντρικής Γραμματείας/Πρωτόκολλο - ΔΚΓΠ**		
	Πεδίο Προσοχής	***Ακούσιο Λάθος Εξουσιοδοτημένου Χρήστη***		
Threat	**(1) Δράστης :** *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	1. Εσωτερικός χρήστης		
	(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*			
	(3) Κίνητρο: *Γιατί το κάνει;*	Ακούσια		
	(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
	(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό θα τροποποιηθεί.		
	(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*	
			Πεδίο Επιπτώσεων	**Αξία** / **Βαθμός**
	Η απώλεια ακεραιότητας των ΔΚΓΠ δεν επιφέρει σοβαρά προβλήματα στη διαχείριση του νοσοκομείου.μπορούν.		Φήμη και εμπιστοσύνη πελατών (4)	- / -
			Οικονομικά (2)	1 / 2
			Παραγωγικότητα (3)	- / -
			Ασφάλεια και Υγεία (5)	- / -
			Πρόστιμα και Νομικές Κυρώσεις (1)	- / -
				Relative Risk Score / **2**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	Αποδοχή	Ελαχιστοποίηση	Μεταβίβαση
Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:			
Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*		
Εφαρμογή	Η εφαρμογή θα έχει διαδικασίες ελέγχου εισαγωγής δεδομένων Η εφαρμογή θα έχει διαδικασίες ελέγχου διπλοεγγραφών		

Allegro Worksheet 8	ΠΡΟΦΙΛ ΚΡΙΣΙΜΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ (IT) Α	
(1) Κρίσιμο Αγαθό: *Ποιο είναι το κρίσιμο IT αγαθό;*	**(2) Αιτιολόγηση της Επιλογής:** *Γιατί το IT αγαθό είναι σημαντικό για τον οργανισμό;*	**(3) Περιγραφή:** *Ποια είναι η συμφωνημένη περιγραφή του IT αγαθού;*
Δεδομένα Εξυπηρετητή (DC) - ΔΕ	Α. Είναι απαραίτητα για τη δικτυακές υπηρεσίες του νοσοκομείου, οπότε χωρίς αυτά καμιά εργασία δεν μπορεί να εκτελεστεί	Τα ΔΕ είναι απαραίτητο για διασύνδεση των χρηστών στο δίκτυο αλλά και στο διαδίκτυο. Περιλαμβάνουν τα Active Directory, Domain Controller.
(4) Ιδιοκτήτης/τες: *Σε ποιους ανήκει το IT αγαθό;*		
- ΤΠΟ		
(5) Απαιτήσεις Ασφάλειας: *Ποιες είναι οι απαιτήσεις ασφάλειας για το IT αγαθό;*		
❑ **Εμπιστευτικότητα (Confidentiality)**	Μόνο εξουσιοδοτημένο προσωπικό του νοσοκομείου μπορεί να δει το αγαθό ως εξής:	Τα ΔΕ μπορεί να δει το προσωπικό του ΤΠΟ
	Μόνο εξουσιοδοτημένο προσωπικό των παρόχων μπορεί να δει το αγαθό ως εξής:	Τα ΔΕ μπορεί να δει το προσωπικό της εταιρείας που είναι υπεύθυνη για τη συντήρηση του server
❑ **Ακεραιότητα (Integrity)**	Μόνο εξουσιοδοτημένο προσωπικό του νοσοκομείου μπορεί να τροποποιήσει το αγαθό ως εξής:	Η διαχείριση των ΔΕ (Εισαγωγή, Διαγραφή, Τροποποίηση) θα γίνεται από εξουσιοδοτημένο προσωπικό του ΤΠΟ.
	Μόνο εξουσιοδοτημένο προσωπικό του παρόχου μπορεί να τροποποιήσει το αγαθό ως εξής:	Η διαχείριση των ΔΕ (Εισαγωγή, Διαγραφή, Τροποποίηση) μπορεί να γίνει από εξουσιοδοτημένο προσωπικό των παρόχων: - Πάροχος Συντήρησης server
❑ **Διαθεσιμότητα (Availability)**	Το εξουσιοδοτημένο προσωπικό πρέπει να έχει πρόσβαση το αγαθό ως εξής:	Τα ΔΕ πρέπει να είναι διαθέσιμα στα παρακάτω τμήματα για τις ημέρες λειτουργίας τους: - Τ.Π.Ο.
	Το αγαθό πρέπει να είναι διαθέσιμο για **24** ώρες, **7** μέρες/εβδομάδα, **52** εβδομάδες/χρόνο.	Τα ΔΕ πρέπει να είναι διαθέσιμο όλο το 24ωρο.
❑ **Άλλο**	Το αγαθό υπόκειται σε νόμους για την ασφάλεια ως εξής:	
(6) Σημαντικότερες Απαιτήσεις Ασφάλειας: *Ποιες είναι οι σημαντικότερες απαιτήσεις ασφάλειας για το IT αγαθό;*		
❑ Εμπιστευτικότητα	❑ Ακεραιότητα	✓ **Διαθεσιμότητα** ❑ Άλλο

Allegro Worksheet 9a	ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (ΤΕΧΝΙΚΟ)
ΕΣΩΤΕΡΙΚΟ	
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΕΚΤΗ	ΙΔΙΟΚΤΗΤΗΣ(ΤΕΣ)

Εξυπηρετητής Domain Controller	Τ.Π.Ο.
ΕΞΩΤΕΡΙΚΟ	
Περιγραφη Περιεκτη	**Ιδιοκτητησ(τεσ)**

Allegro Worksheet 9b	**ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ** (Φυσικο)
ΕΣΩΤΕΡΙΚΟ	
Περιγραφη Περιεκτη	Ιδιοκτητησ(τεσ)
Αντίγραφα ασφάλειας σε κασέτα	Τ.Π.Ο.
ΕΞΩΤΕΡΙΚΟ	
Περιγραφη Περιεκτη	Ιδιοκτητησ(τεσ)

Allegro Worksheet 9c	**ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ IT ΑΓΑΘΟΥ (ΑΝΘΡΩΠΟΙ)**
ΕΣΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΟΝΟΜΑ΄Η ΡΟΛΟΣ/ΑΡΜΟΔΙΟΤΗΤΑ	**ΤΜΗΜΑ/ΜΟΝΑΔΑ**
Προσωπικό ΤΠΟ	ΤΠΟ
ΕΞΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΑΝΑΔΟΧΟΣ, ΠΡΟΜΗΘΕΥΤΗΣ, ΚΛΠ.	**ΟΡΓΑΝΙΣΜΟΣ**
Προσωπικό Παρόχου Συντήρησης Server	Πάροχος Συντήρησης Server

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**		
Information Asset Risk	**Threat**	**IT Αγαθό**	**Δεδομένα Εξυπηρετητή - ΔΕ**	
		Πεδίο Προσοχής	***Αστοχία Υλικού***	
		(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*		
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*		
		(3) Κίνητρο: *Γιατί το κάνει;*		
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**	
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό δεν είναι Διαθέσιμο στους χρήστες	
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια** **Χαμηλή**

(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*	**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
	Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
Η απώλεια Διαθεσιμότητας των ΔΕ επιφέρει σοβαρά προβλήματα στη διαχείριση του νοσοκομείου.	Φήμη και εμπιστοσύνη πελατών (4)	1	4

		Οικονομικά (2)	2	4
		Παραγωγικότητα (3)	3	9
		Ασφάλεια και Υγεία (5)	1	5
		Πρόστιμα και Νομικές Κυρώσεις (1)	-	-
			Relative Risk Score	**22**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αναβολή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εξυπηρετητές	Συμβόλαιο συντήρησης Σχέδιο Ανάκαμψης από Καταστροφή Αντίγραφα Ασφάλειας Έλεγχος Πρόσβασης

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**			
Information Asset Risk		**IT Αγαθό**	**Δεδομένα Εξυπηρετητή - ΔΕ**		
		Πεδίο Προσοχής	***Ακούσιο Λάθος Εξουσιοδοτημένου Χρήστη***		
	Threat	**(1) Δράστης :** *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	1. Εσωτερικός χρήστης		
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*			
		(3) Κίνητρο: *Γιατί το κάνει;*	Ακούσια		
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Το αγαθό θα τροποποιηθεί.		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
			Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
	Η απώλεια ακεραιότητας των ΔΕ δεν επιφέρει σοβαρά προβλήματα στη διαχείριση του νοσοκομείου.		Φήμη και εμπιστοσύνη πελατών (4)	-	-
			Οικονομικά (2)	-	-
			Παραγωγικότητα (3)	1	3
			Ασφάλεια και Υγεία (5)	-	-

		Πρόστιμα και Νομικές Κυρώσεις (1)	-	-
			Relative Risk Score	**3**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αποδοχή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:

Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εξυπηρετητής	Αντίγραφα ασφάλειας

Allegro Worksheet 10	**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**			
Information Asset Risk / **Threat**	**IT Αγαθό**	**Δεδομένα Εξυπηρετητή - ΔΕ**		
	Πεδίο Προσοχής	***Μη εξουσιοδοτημένη πρόσβαση στο Υποσύστημα***		
	(1) Δράστης : *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	1. Εσωτερικός χρήστης που έχει υποκλέψει συνθηματικά 2. Εξωτερικός χρήστης που έχει αποκτήσει πρόσβαση μέσω του δικτύου και έχει ανακαλύψει συνθηματικά		
	(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	1. Ο εσωτερικός χρήστης εκμεταλλευόμενος αμέλεια στη φύλαξη των συνθηματικών ενός νόμιμου χρήστη 2. Ο εξωτερικός χρήστης εκμεταλλευόμενος αδυναμία στην ασφάλεια του δικτύου		
	(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος		
	(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
	(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Επηρεάζονται η Ακεραιότητα και η Διαθεσιμότητα		
	(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*	
			Πεδίο Επιπτώσεων	**Αξία** / **Βαθμός**
	Η απώλεια διαθεσιμότητας και ακεραιότητας των ΔΕ δεν επιφέρει σοβαρά προβλήματα στη διαχείριση του νοσοκομείου.		Φήμη και εμπιστοσύνη πελατών (4)	1 / 4
			Οικονομικά (2)	- / -
			Παραγωγικότητα (3)	- / -
			Ασφάλεια και Υγεία (5)	- / -
			Πρόστιμα και Νομικές Κυρώσεις (1)	- / -
			Relative Risk Score	**4**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αποδοχή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:	
Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εξυπηρετητές	Έλεγχος πρόσβασης Παρακολούθηση τρίτων που έχουν πρόσβαση Αντίγραφα ασφάλειας

Allegro Worksheet 10		**ΚΙΝΔΥΝΟΣ ΓΙΑ ΤΟ IT ΑΓΑΘΟ**			
Information Asset Risk		**IT Αγαθό**	***Δεδομένα Εξυπηρετητή - ΔΕ***		
		Πεδίο Προσοχής	***Εισαγωγή Κακόβουλου Κώδικα***		
	Threat	**(1) Δράστης :** *Ποιος θα μπορούσε να εκμεταλλευτεί την αδυναμία*	1. Εσωτερικός χρήστης 2. Εξωτερικός χρήστης που έχει αποκτήσει πρόσβαση μέσω του δικτύου		
		(2) Τρόποι/Μέσα: *Πως μπορεί ο δράστης να το πετύχει, τι θα έκανε;*	1. Ο εσωτερικός χρήστης με την πρόσβαση στο ΠΣ 2. Ο εξωτερικός χρήστης εκμεταλλευόμενος αδυναμία στην ασφάλεια του δικτύου		
		(3) Κίνητρο: *Γιατί το κάνει;*	Προσωπικό όφελος		
		(4) Αποτέλεσμα: *Ποια επίδραση θα έχει στο αγαθό;*	**Αποκάλυψη** **Καταστροφή** **Τροποποίηση** **Διακοπή**		
		(5) Απαιτήσεις Ασφάλειας: *Πως παραβιάζονται οι απαιτήσεις ασφάλειας του αγαθού;*	Επηρεάζονται η Ακεραιότητα και η Διαθεσιμότητα		
		(6) Πιθανότητα: *Ποια είναι η πιθανότητα να συμβεί η απειλή;*	**Υψηλή**	**Μέτρια**	**Χαμηλή**
	(7) Συνέπειες: *Ποιες είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού εξαιτίας της παραβίασης των απαιτήσεων ασφάλειας του αγαθού;*		**(8) Βαρύτητα:** *Πόσο σοβαρές είναι οι συνέπειες στον οργανισμό ή στον ιδιοκτήτη του αγαθού ανά πεδίο επιπτώσεων;*		
			Πεδίο Επιπτώσεων	**Αξία**	**Βαθμός**
	Η απώλεια διαθεσιμότητας για μικρό χρονικό διάστημα των ΔΕ δεν επιφέρει σοβαρά προβλήματα στη διαχείριση του νοσοκομείου.		Φήμη και εμπιστοσύνη πελατών (4)	1	4
			Οικονομικά (2)	1	2
			Παραγωγικότητα (3)	2	6
			Ασφάλεια και Υγεία (5)	-	-
			Πρόστιμα και Νομικές Κυρώσεις (1)	-	-
				Relative Risk Score	**12**

(9) Ελαχιστοποίηση Κινδύνου: *Επιλογή ενεργειών αντιμετώπισης του κινδύνου, βασισμένη στη συνολική βαθμολογία του κινδύνου.*

Αποδοχή	**Αποδοχή**	**Ελαχιστοποίηση**	**Μεταβίβαση**

Για τους κινδύνους που πρέπει να ελαχιστοποιηθούν, θα εκτελεστούν τα παρακάτω αντίμετρα:	
Περιέκτης εφαρμογής αντίμετρων;	*Ποιοι είναι οι διαχειριστικοί, τεχνικοί και φυσικοί έλεγχοι που θα εφαρμοστούν στον περιέκτη;*
Εξυπηρετητές	Έλεγχος πρόσβασης Παρακολούθηση τρίτων που έχουν πρόσβαση Αντίγραφα ασφάλειας Πρόγραμμα προστασίας από κακόβουλο λογισμικό