Τμήμα Πληροφορικής
Εαρινό εξάμηνο 2022-23
Dr. Γεωργία Λύκου,
B.Sc., MBA, M.Sc., Ph.D.
e-mail: lykoug@aueb.gr
website: www.infosec.aueb.gr

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Μελέτη Περίπτωσης Ανάλυσης Επικινδυνότητας Πληροφοριακών Συστημάτων σε Μικροβιολογικό Εργαστήριο

ΓΡΑΠΤΗ ΕΡΓΑΣΙΑ

Η ανάλυση επικινδυνότητας των Πληροφοριακών Συστημάτων αποτελεί έναν πρότυπο έλεγχο των υποδομών, διαδικασιών και λογισμικού κάθε οργανισμού προκειμένου να εντοπιστούν πιθανές απειλές, υπάρχουσες ευπάθειες στην ασφάλειά του και να υπολογιστούν οι συνέπειες από την πραγματοποίηση μιας υπάρχουσας απειλής.

Ένα **σύγχρονο μικροβιολογικό εργαστήριο** χρειάζεται την υλοποίηση ενός Πληροφοριακού Συστήματος για την καταγραφή, παρακολούθηση, λειτουργία, καθώς και την καλύτερη εξυπηρέτηση των πελατών/ασθενών που διαχειρίζεται.

Στην παρούσα εργασία καλείστε να εκπονήσετε **μία ολοκληρωμένη πρόταση ενός σχεδίου ασφαλείας** για ένα νέο μικροβιολογικό εργαστήριο που περιγράφεται παρακάτω, με βάση την επιτόπια επισκόπηση των εγκαταστάσεων και των παρατηρήσεων που κατέγραψε ο αρμόδιος εμπειρογνώμων. Στηριχτείτε στα σχέδια και στην τοπολογία δικτύου που σας δίνεται παρακάτω, καθώς και στις παρατηρήσεις που εντοπίστηκαν κατά την επιτόπια επίσκεψή σας.

Το σχέδιο ασφάλειας που θα παραδώσετε πρέπει **να παρουσιάσει τα βήματα ανάλυσης επικινδυνότητας**, όπου εντοπίζονται οι πιθανές απειλές και ευπάθειες του συστήματος, η αποτίμηση της επικινδυνότητας και κατόπιν προτείνονται τα οργανωτικά και τεχνικά μέτρα που πρέπει να ληφθούν για τη διαχείριση της επικινδυνότητας και του εναπομένοντος κινδύνου.

Σας δίνονται τα ακόλουθα:

1. Σύντομη περιγραφή του Εργαστηρίου, (*επισυναπτόμενη στην εκφώνηση της Εργασίας*) με τις παρατηρήσεις, που κατέγραψε σε επιτόπιο έλεγχο ο επιθεωρητής ασφάλειας. Επίσης δίδεται η **κάτοψη του εργαστηρίου** και το **διάγραμμα δικτύου** Πληροφοριακών συστημάτων, που αποτύπωσε ο επιθεωρητής ασφάλειας.

2. **Αρχείο Excel με ονόμα: «MicroLab_Asset Inventory_2023»** με την αρχική καταγραφή των αγαθών, που εντοπίστηκαν από τον επιθεωρητή ασφαλείας**.**
3. **Αρχείο Excel με ονόμα: «ISO27k FMEA[1] - Risk Assessment_2023.xlsx)** που παρέχει μέσα όλες τις αναγκαίες πληροφορίες για την διεξαγωγή της προσομοίωσης ανάλυσης επικινδυνότητας **(**κλίμακες **Impact, Likelihood, Vulnerability** καθώς και **Risk Assessment** φύλλο με formula υπολογισμού για να συμπληρώσετε την ανάλυση σας).
4. **Υπόδειγμα Εργασίας (Template Εργασίας ΑΠΣ_2023**), με περιεχόμενα και βασικά κεφάλαια, που πρέπει να περιλαμβάνει η παραδοτέα εργασία σας. Η **μη τήρηση του template θα οδηγήσει σε απώλεια 15% του συνολικού βαθμού της εργασίας.**

Οδηγίες για την εκπόνηση της εργασίας:

- Το κείμενο που θα παραδώσετε πρέπει να ακολουθεί την κατάλληλη δομή, προσεκτική μορφοποίηση και αυτοματοποιημένα περιεχόμενα, όπως σας δίνονται στο υπόδειγμα του σχεδίου ασφάλειας: **Template Εργασίας ΑΠΣ_2023.docx**.
- Μπορείτε να κάνετε οποιαδήποτε παραδοχή χρειαστείτε αρκεί να είναι επαρκώς τεκμηριωμένη. Επίσης, **πρέπει να προσθέσετε τουλάχιστον άλλα 3 αγαθά** τα οποία θα εντάξετε ρητά μετά από έρευνα, εύλογη σκέψη και τεκμηρίωση και εφόσον δεν παραβλάπτεται η γενικότητα των μελετών περιπτώσεων.
- Πρέπει να καταθέσετε: 1) Το προτεινόμενο **Σχέδιο ασφάλειας σε μορφή PDF** με βάση το υπόδειγμα και 2) Το αρχείο **ISO27k FMEA - Risk Assessment_2023.xlsx** συμπληρωμένο με την αποτίμηση που θα πραγματοποιήσατε και τεκμηριώνει τις προτάσεις σας παρουσιάζοντας όλους τις αλυσίδες Αγαθών-Επιπτώσεων-Πιθανότητας και Ευπαθειών που εντοπίσατε.

Διαδικαστικές διευκρινίσεις:

Παραδοτέα: **Συμπιεσμένο Αρχείο ZIP** που θα περιλαμβάνει 1) το κείμενο τεκμηρίωσης σε μορφή pdf, με χρήση του προτεινόμενου template και των βιβλιογραφικών πηγών που χρησιμοποιήθηκαν, 2) το αρχείο αποτίμησης επικινδυνότητας με βάση το πρότυπο αρχείο ISO27k FMEA. Το όνομα του αρχείου ZIP θα είναι οι Αρ. Μητρώου των φοιτητών που μετέχουν στην ομάδα εργασίας (π.χ. 31800XX_31900XX - ***!! ΠΡΟΣΟΧΗ ΣΤΗΝ ΟΡΘΗ ΑΝΑΦΟΡΑ ΑΜ & ΟΝΟΜΑΤΩΝ!!***

Υποβολή: Ηλεκτρονική υποβολή της εργασίας στο E-Class, μέχρι τη **Πέμπτη, 4 Μαΐου 2023, ώρα 23:00**.

Εκπόνηση: Ανά ομάδες, αποτελούμενες από **2-3 φοιτητές**.(*δεν θα γίνουν δεκτές εργασίες που εκπονήθηκαν από έναν μόνο φοιτητή*).

Βαρύτητα: Ποσοστό 30% του συνολικού βαθμού. Επιτυχόντες στο μάθημα είναι όσοι αξιολογηθούν με ≥5.0 και στην εργασία και στο εργαστήριο και στην τελική γραπτή εξέταση, που θα ακολουθήσουν.

Κατοχύρωση: Ο βαθμός της εργασίας κατοχυρώνεται, αποκλειστικά και μόνον, για τις (κανονικές) εξεταστικές περιόδους Ιουνίου και Σεπτέμβρη 2023.

Καλή επιτυχία!

[1] Η μέθοδος FMEA (Failure Mode and Effects Analysis) χρησιμοποιείται για την αποτίμηση κινδύνου σε κάθε αγαθό (*σύστημα ή διαδικασία*) σε περίπτωση αστοχίας αυτού (Failure), εξετάζοντας τις δυσμενείς επιπτώσεις, που επιφέρει στον οργανισμό, χωρίς την αποτίμηση της αξίας κάθε αγαθού.
For more info visit ISO27k Forum: https://www.iso27001security.com/index.html

Σύντομη Περιγραφή του Εργαστηρίου

Το εργαστήριο βρίσκεται σε ισόγειο εμπορικού κέντρου, όπου η πρόσοψη βλέπει σε κεντρικό δρόμο της Αθήνας, ενώ η πίσω όψη σε πολυσύχναστο πεζόδρομο.

Το εργαστήριο διαθέτει δίκτυο ηλεκτρονικών υπολογιστών και αναλυτών σύγχρονης τεχνολογίας για την καλύτερη εξυπηρέτηση των πελατών του. Το εργαστήριο είναι αυτοματοποιημένο στα περισσότερα στάδια διενέργειας των διαγνωστικών εξετάσεων, όπου με τη χρήση barcode ταυτοποιούνται τα δείγματα από τη στιγμή της δειγματοληψίας των ασθενών έως και την εξαγωγή των αποτελεσμάτων.

Η επικοινωνία των μικροβιολογικών αναλυτών του εργαστηρίου γίνεται δικτυακά με το πληροφοριακό σύστημα του εργαστηρίου κι επιτρέπει την άμεση πραγματοποίηση των απαιτούμενων αναλύσεων και την αυτόματη καταχώρηση των αποτελεσμάτων.

Το ιστορικό των εξετάσεων, το αρχείο των πελατών, προμηθευτών και υπαλλήλων διατηρείται σε βάση δεδομένων της ORACLE στον Database server του εργαστήριου με στόχο την ηλεκτρονική διανομή αποτελεσμάτων και αναφορών, την στατιστική ανάλυση και επιτήρηση, καθώς και την εκτύπωση νέων και παλαιότερων αποτελεσμάτων των ασθενών. Το αρχείο των ασθενών/πελατών, προμηθευτών, και υπαλλήλων διατηρείται επίσης αρχειοθετημένο και σε φυσικά αρχεία σε ερμάρια κρεμαστών φακέλων εντός του εργαστηρίου για την διευκόλυνση του έργου της γραμματείας.

Στον Βοηθητικό χώρο φυλάσσονται κάποιες χημικές ουσίες, που απαιτούνται για τα αντιδραστήρια του εργαστηρίου. Στον χώρο υπάρχει αισθητήρας πυρανίχνευσης και φορητός πυροσβεστήρας ξηράς κόνεως για την προστασία έναντι κινδύνου πυρός από εύφλεκτα υλικά και τοξικές ουσίες, ενώ συνήθως η πόρτα παραμένει μισάνοικτη για τον αερισμό του χώρου.

Γίνεται λήψη αντιγράφων ασφαλείας κάθε εβδομάδα για την προστασία των δεδομένων σε περίπτωση που καταστραφεί ή κλαπεί ο υπολογιστής. Τα αντίγραφα ασφαλείας φυλάσσονται στο γραφείο του Ιατρού.

Τα αποτελέσματα των εξετάσεων/αναλύσεων δίνονται αυθημερόν στους ασθενείς ή αποστέλλονται με fax ή e-mail στον ίδιο τον ασθενή ή τον θεράποντα γιατρό του. Επιπρόσθετα, οι ασθενείς μπορούν να λάβουν τα αποτελέσματα μέσω internet, εφόσον συνδεθούν στον διαδικτυακό ιστότοπο του μικροβιολογικού εργαστηρίου. Το website έχει σχεδιαστεί και κατασκευαστεί από τον ιδιοκτήτη/ιατρό του εργαστηρίου με χρήση της εφαρμογής JOOMLA.

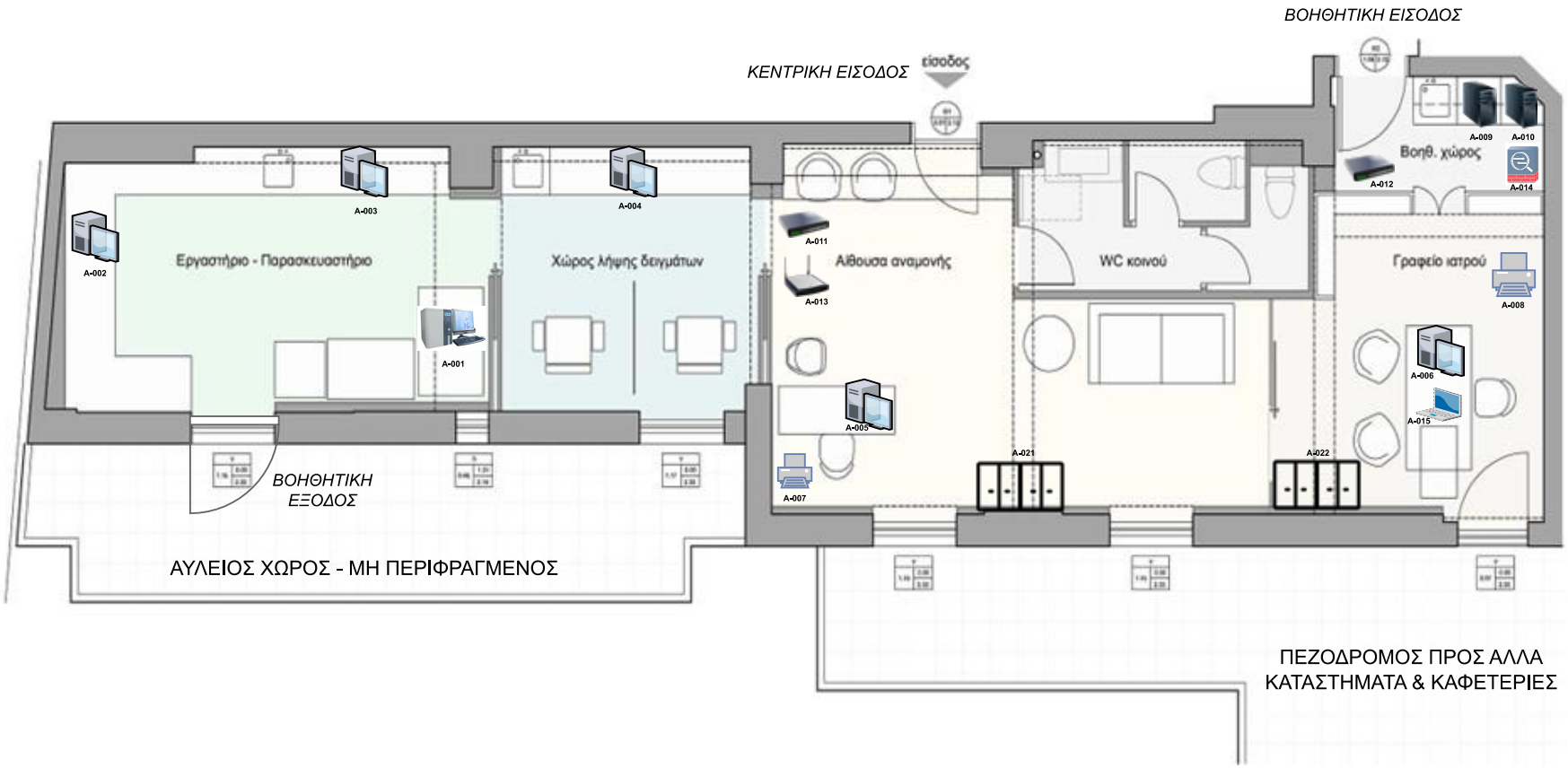
«*Το Εργαστήριο συλλέγει προσωπικές πληροφορίες των ασθενών για τη διενέργεια μικροβιολογικών εξετάσεων και συμμορφώνεται με τις υποχρεώσεις για την προστασία δεδομένων προσωπικού χαρακτήρα και τη διαχείριση των προσωπικών δεδομένων*», όπως δήλωσε ο υπεύθυνος επεξεργασίας.

Σε ορισμένες περιπτώσεις, το Εργαστήριο ενδέχεται να μοιραστεί τα προσωπικά δεδομένα με συνεργαζόμενους παρόχους υπηρεσιών για την καλύτερη εξυπηρέτηση των ασθενών, αλλά δεν λαμβάνει πάντα γραπτή συναίνεση των ασθενών για το σκοπό αυτό.

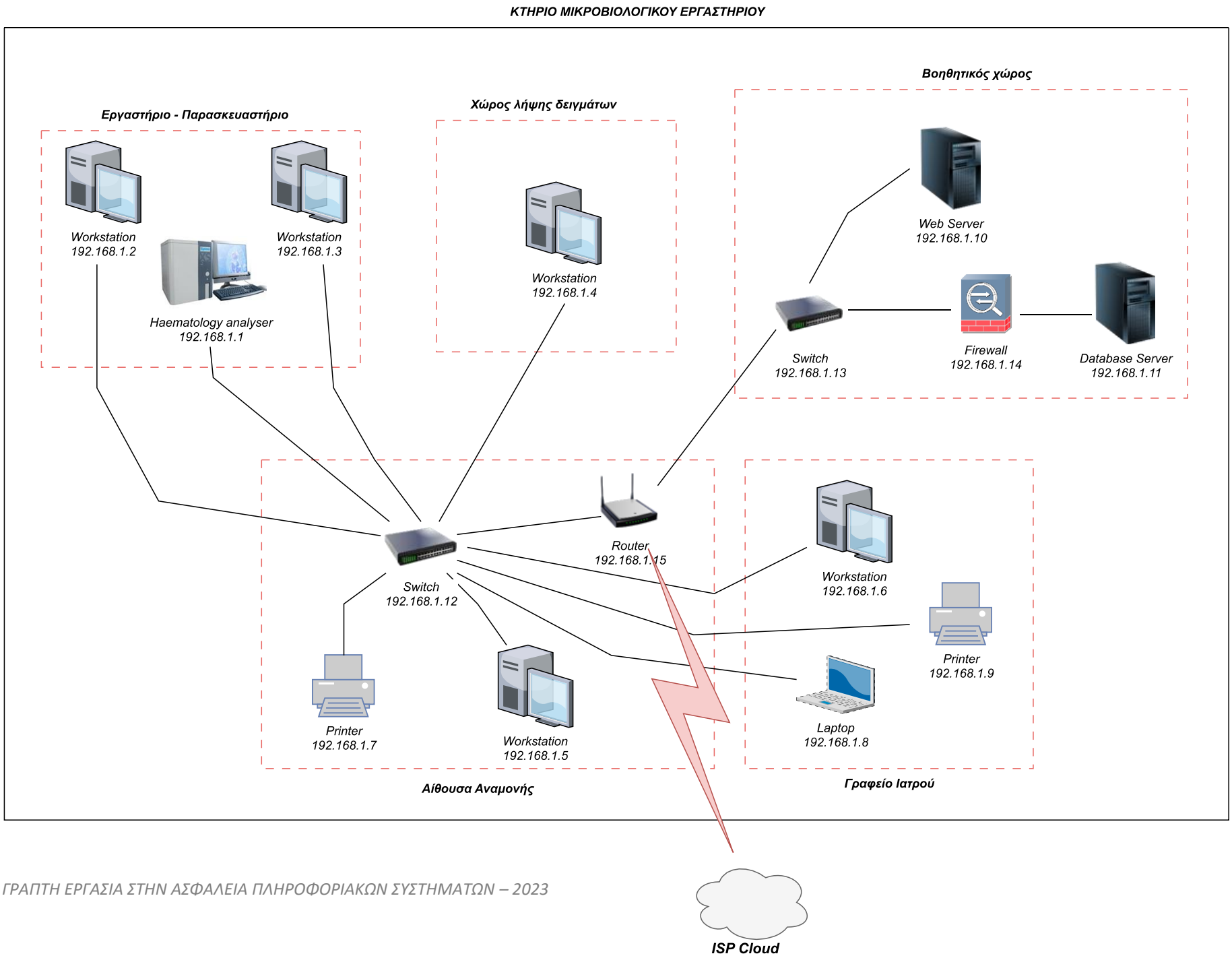
Παρότι ο υπεύθυνος του Εργαστηρίου δήλωσε ότι εφαρμόζει πολιτικές και διαδικασίες τεχνικής και οργανωτικής ασφαλείας για την προστασία των προσωπικών δεδομένων και πληροφοριών από απώλεια, κακόβουλη χρήση, μεταβολή ή καταστροφή, ο επιθεωρητής διαπίστωσε σημαντικά σφάλματα και παραλείψεις στην ασφάλεια των ΠΣ. *(που θα αποτυπωθούν στο Σχέδιο Ασφαλείας που θα υποβάλλετε στα πλαίσια αυτή της εργασίας)*

Παρακάτω παρουσιάζεται η κάτοψη των χώρων του εργαστηρίου με την καταγραφή που εξοπλισμού, καθώς και το δικτυακό διάγραμμα συνδέσεων των πληροφοριακών συστημάτων όπως καταγράφηκαν από τον επιθεωρητή ασφαλείας που διεξήγαμε την επιτόπια καταγραφή.

ΠΟΛΥΣΥΧΝΑΣΤΟΣ ΔΡΟΜΟΣ



ΚΑΤΟΨΗ


ΚΤΗΡΙΟ ΜΙΚΡΟΒΙΟΛΟΓΙΚΟΥ ΕΡΓΑΣΤΗΡΙΟΥ
Εργαστήριο - Παρασκευαστήριο
Workstation
192.168.1.2
Workstation
192.168.1.3
Haematology analyser
192.168.1.1
Χώρος λήψης δειγμάτων
Workstation
192.168.1.4
Βοηθητικός χώρος
Web Server
192.168.1.10
Switch
192.168.1.13
Firewall
192.168.1.14
Database Server
192.168.1.11
Router
192.168.1.15
Switch
192.168.1.12
Printer
192.168.1.7
Workstation
192.168.1.5
Αίθουσα Αναμονής
Workstation
192.168.1.6
Printer
192.168.1.9
Laptop
192.168.1.8
Γραφείο Ιατρού
ISP Cloud