megalab
ΔΙΑΓΝΩΣΤΙΚΑ ΕΡΓΑΣΤΗΡΙΑ

Πολιτική Ασφάλειας Πληροφοριών και Δεδομένων

Στοιχεία Έγκρισης

Όνομα	Θέση	Υπογραφή	Ημερομηνία
ΔΗΜΟΤΣΑΝΤΟΣ ΓΕΩΡΓΙΟΣ	ΠΡΟΕΔΡΟΣ Κ/Δ ΔΙΟΙΚΗΤΙΚΟΥ ΣΥΜΒΟΥΛΙΟΥ		16/09/2023.

1 Εισαγωγή

Η παρούσα Πολιτική καταγράφει και καθορίζει τις γενικές αρχές για την ασφάλεια των πληροφοριών και δεδομένων στις Εταιρίες «**MEGALAB ΙΔΙΩΤΙΚΑ ΔΙΑΓΝΩΣΤΙΚΑ ΕΡΓΑΣΤΗΡΙΑ ΑΝΩΝΥΜΗ ΕΤΑΙΡΙΑ**», «**MEGALAB ΡΟΔΟΥ ΔΙΑΓΝΩΣΤΙΚΟ ΕΡΓΑΣΤΗΡΙΟ-ΚΕΝΤΡΟ ΑΝΩΝΥΜΗ ΕΤΑΙΡΙΑ**» και «**MEGALAB ΑΙΓΑΛΕΩ ΔΙΑΓΝΩΣΤΙΚΑ ΕΡΓΑΣΤΗΡΙΑ ΑΝΩΝΥΜΗ ΕΤΑΙΡΙΑ**» (εφεξής **MEGALAB ΔΙΑΓΝΩΣΤΙΚΑ ΕΡΓΑΣΤΗΡΙΑ** ή τα Εργαστήρια).

Ως σύγχρονη επιχείρηση με προσανατολισμό προς το μέλλον, τα **MEGALAB ΔΙΑΓΝΩΣΤΙΚΑ ΕΡΓΑΣΤΗΡΙΑ** αναγνωρίζουν ως πρωταρχικό στόχο τους την ανάγκη να διασφαλίσουν την ομαλή και αδιάλειπτη λειτουργία τους προς όφελος των πελατών τους, των μετόχων τους και άλλων ενδιαφερόμενων μερών.

Προκειμένου να εξασφαλίζουν ένα τέτοιο επίπεδο συνεχούς λειτουργίας, τα **MEGALAB ΔΙΑΓΝΩΣΤΙΚΑ ΕΡΓΑΣΤΗΡΙΑ** έχουν εφαρμόσει ένα σύνολο Πολιτικών και σημείων ελέγχων για την ασφάλεια και προστασία των πληροφοριών και δεδομένων που διαχειρίζονται, καθώς και για τον εντοπισμό και την αντιμετώπιση πιθανών κινδύνων που σχετίζονται με τη διαχείριση πληροφοριών και δεδομένων από τα Εργαστήρια.

2 Σκοπός

Βασικός σκοπός της Πολιτικής Ασφάλειας Πληροφοριών και Δεδομένων είναι να εξασφαλίσει ισχυρή προστασία για το σύνολο των πληροφοριακών περιουσιακών στοιχείων των **MEGALAB ΔΙΑΓΝΩΣΤΙΚΩΝ ΕΡΓΑΣΤΗΡΙΩΝ** (τόσο των πληροφοριών και δεδομένων που διαχειρίζονται τα Εργαστήρια, όσο και των πληροφοριακών υποδομών και του εξοπλισμού τους) από όλες τις εσωτερικές, εξωτερικές, εκούσιες ή ακούσιες απειλές.

Επιμέρους στόχοι της ασφάλειας πληροφοριών είναι:

- Η προστασία των πληροφοριών και δεδομένων από οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση
- Η διασφάλιση της εμπιστευτικότητας πληροφοριών και δεδομένων
- Η διατήρηση της ακεραιότητας πληροφοριών και δεδομένων
- Η συνεχής διαθεσιμότητα πληροφοριών και δεδομένων
- Η συμμόρφωση των Εργαστηρίων με νομοθετικές και ρυθμιστικές απαιτήσεις
- Η ανάπτυξη, τήρηση και δοκιμή Σχεδίων Επιχειρησιακής Συνέχειας
- Η εκπαίδευση του ανθρώπινου δυναμικού των Εργαστηρίων στην ασφάλεια των πληροφοριών και τη σημασία της
- Η έγκαιρη και πλήρης διερεύνηση και εκτίμηση περιστατικών ασφαλείας (πραγματικών ή δυνητικών)

Μέσω της ασφάλειας των πληροφοριών διασφαλίζονται -ενδεικτικά μεταξύ άλλων- θέματα όπως:

- Η αδιάλειπτη λειτουργία των Εργαστηρίων και η συνεχής προμήθεια υπηρεσιών στους πελάτες τους
- Η κερδοφορία των Εργαστηρίων
- Η συμμόρφωση με νομικές και κανονιστικές απαιτήσεις

3 Πεδίο Εφαρμογής

Η Πολιτική Ασφάλειας Πληροφοριών και Δεδομένων εφαρμόζεται από και ισχύει για όλο το ανθρώπινο δυναμικό των Εργαστηρίων (συμπεριλαμβανομένων των μελών της Διοίκησης, διευθυντών, εργαζομένων, προμηθευτών και άλλων τρίτων που έχουν πρόσβαση στα συστήματα των Εργαστηρίων), καθώς και για όλο τον εξοπλισμό, τα συστήματα, τους ανθρώπους και τις διαδικασίες που αποτελούν την ευρύτερη πληροφοριακή δομή των Εργαστηρίων.

Τα παρακάτω αναφερόμενα έγγραφα αποτελούν το σύνολο των Πολιτικών Πληροφορικής Ασφαλείας των Εργαστηρίων, υποστηρίζουν την παρούσα Πολιτική Ασφάλειας Πληροφοριών και Δεδομένων και καθορίζουν τον επιμέρους τρόπο εφαρμογής της:

- *Πολιτική Ορθής Χρήσης*
- *Πολιτική Φορητών Συσκευών*
- *Πολιτική Ελέγχου Πρόσβασης*
- *Πολιτική Κρυπτογράφησης*
- *Πολιτική Φυσικής Ασφάλειας*
- *Πολιτική κατά των κακόβουλων προγραμμάτων (anti-malware)*
- *Πολιτική Ασφάλειας Δικτύου*
- *Πολιτική Ηλεκτρονικών Μηνυμάτων*
- *Πολιτική Cloud Computing*
- *Πολιτική Λήψης Αντιγράφων Ασφαλείας (Back-up)*
- *Πολιτική Τηλε-εργασίας*
- *Πολιτική Λειτουργίας Συστήματος Βινετοεπιτήρησης (CCTV)*
- *Πολιτική Προστασίας Δεδομένων*

4 Αρμοδιότητες και Ευθύνες

4.1 Διοίκηση

Η Διοίκηση των **MEGALAB ΔΙΑΓΝΩΣΤΙΚΩΝ ΕΡΓΑΣΤΗΡΙΩΝ** δεσμεύεται να μεριμνά συνεχώς για την ασφάλεια των πληροφοριών και δεδομένων που διαχειρίζονται τα Εργαστήρια και για την παροχή όλων των απαραίτητων πόρων και μέσων για την εφαρμογή της παρούσας και των επιμέρους Πολιτικών Ασφαλείας.

Βασικές αρμοδιότητές της για την επίτευξη του σκοπού αυτού είναι:

- Η διαμόρφωση, έγκριση και ανασκόπηση της γενικής Πολιτικής Ασφάλειας Πληροφοριών και Δεδομένων των Εργαστηρίων
- Η έγκριση και η ανασκόπηση του συνόλου των Πολιτικών Πληροφορικής Ασφαλείας των Εργαστηρίων και των συνοδευτικών υποστηρικτικών εγγράφων τους (Διαδικασίες, Οδηγίες Εργασίας, Έντυπα κλπ.)
- Η έγκριση των Σχεδίων Διαχείρισης των Κινδύνων και των Σχεδίων Διαχείρισης Εκτάκτων Αναγκών (Επιχειρησιακή Συνέχεια)
- Η εξασφάλιση των υλικοτεχνικών πόρων που απαιτούνται για την εφαρμογή των αναγκαίων μέτρων με σκοπό την προστασία της ασφάλειας πληροφοριών και δεδομένων
- Η εξασφάλιση των υλικοτεχνικών πόρων που απαιτούνται για την εφαρμογή των αναγκαίων οργανωτικών και τεχνικών μέτρων με σκοπό τη συμμόρφωση των Εργαστηρίων με την ευρύτερη εθνική και ευρωπαϊκή νομοθεσία για την προστασία των δεδομένων προσωπικού χαρακτήρα (Προσωπικά Δεδομένα)
- Η δημιουργία των απαραίτητων συνθηκών στα Εργαστήρια για την κατανόηση από το προσωπικό του ρόλου και των ευθυνών του που συνδέονται με την ασφάλεια της πληροφορίας
- Η μέριμνα για τη συνεχή βελτίωση σε θέματα που αφορούν την ασφάλεια πληροφοριών και δεδομένων
- Η λήψη αποφάσεων για την επιβολή κυρώσεων σε περιπτώσεις πειθαρχικών παραπτωμάτων σε σχέση με την ασφάλεια πληροφοριών και δεδομένων

4.2 Υπεύθυνος Ασφάλειας Πληροφοριών (ΥΑΠ)

Ο Υπεύθυνος Ασφάλειας Πληροφοριών (ΥΑΠ) ορίζεται από τη Διοίκηση των **MEGALAB ΔΙΑΓΝΩΣΤΙΚΩΝ ΕΡΓΑΣΤΗΡΙΩΝ**, αναφέρεται απευθείας σε αυτή για όλα τα θέματα που σχετίζονται με την ασφάλεια των Πληροφοριών και έχει τις παρακάτω αρμοδιότητες:

- Εξέταση των δραστηριοτήτων των Εργαστηρίων που σχετίζονται με την ασφάλεια της πληροφορίας και εντοπισμός των εμπλεκομένων πληροφοριακών περιουσιακών στοιχείων και των κινδύνων που τα απειλούν
- Εποπτεία της διαχείρισης της ασφάλειας πληροφοριών από τα Εργαστήρια
- Συνεργασία με τη Διοίκηση για την ανάπτυξη Πολιτικών Πληροφορικής Ασφάλειας, διαδικασιών και πρότυπων μεθόδων, σύμφωνα με τη γενικής Πολιτική Ασφάλειας Πληροφοριών και Δεδομένων
- Μέριμνα για την εφαρμογή, διατήρηση και αποτελεσματικότητα των Πολιτικών Πληροφορικής Ασφάλειας
- Διενέργεια εσωτερικών επιθεωρήσεων για τον έλεγχο τήρησης των Πολιτικών Πληροφορικής Ασφάλειας
- Ενημέρωση της Διοίκησης για την ανάγκη βελτίωσης ή/και επικαιροποίησης των Πολιτικών Πληροφορικής Ασφάλειας

- Τήρηση και ενημέρωση του καταλόγου πληροφοριακών στοιχείων των Εργαστηρίων και διαβάθμιση της σπουδαιότητάς τους, σε συνεργασία με τα αρμόδια στελέχη
- Εντοπισμός και αξιολόγηση των κινδύνων που απειλούν τα πληροφοριακά αγαθά των Εργαστηρίων, σε συνεργασία με τα αρμόδια στελέχη
- Συνεργασία με τη Διοίκηση για τον καθορισμό των απαραίτητων ελέγχων ή/και μέτρων για την αντιμετώπιση των κινδύνων αναφορικά με την ασφάλεια των πληροφοριών και τον πληροφοριακό εξοπλισμό των Εργαστηρίων
- Παρακολούθηση και ενημέρωση της Διοίκησης για οποιοδήποτε περιστατικό ασφαλείας και ενεργοποίηση του αντίστοιχου σχεδίου και στρατηγικής για την αντιμετώπιση και την αποφυγή επανεμφάνισής του
- Παρακολούθηση της αποτελεσματικότητας των ελέγχων ή/και μέτρων που εφαρμόζονται για την αντιμετώπιση των κινδύνων και σχετική ενημέρωση της Διοίκησης
- Επικοινωνία με εξωτερικούς Φορείς και τρίτα μέρη για θέματα σχετικά με την ασφάλεια των Πληροφοριών
- Συμμετοχή σε Διοικητικά Συμβούλια που αφορούν την ασφάλεια των πληροφοριών
- Μέριμνα για την εκπαίδευση και ευαισθητοποίηση του προσωπικού σχετικά με την ασφάλεια των πληροφοριών και δεδομένων που διαχειρίζονται τα Εργαστήρια και των πληροφοριακών συστημάτων και εξοπλισμού που χειρίζονται οι εργαζόμενοι

4.3 Υπεύθυνος Προστασίας Δεδομένων (DPO)

Ο Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer – DPO) ορίζεται από τη Διοίκηση των **MEGALAB ΔΙΑΓΝΩΣΤΙΚΩΝ ΕΡΓΑΣΤΗΡΙΩΝ**, αναφέρεται απευθείας σε αυτή για όλα τα θέματα που σχετίζονται με την επεξεργασία Προσωπικών Δεδομένων από τα Εργαστήρια και έχει τις παρακάτω αρμοδιότητες:

- Ενημέρωση της Διοίκησης για τις υποχρεώσεις των Εργαστηρίων που απορρέουν από τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) και την ευρύτερη εθνική και ευρωπαϊκή νομοθεσία περί προστασίας δεδομένων
- Παρακολούθηση της συμμόρφωσης των Εργαστηρίων, των διαδικασιών και πολιτικών που αυτά εφαρμόζουν με τις διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και των εθνικών και ευρωπαϊκών διατάξεων σχετικά με την προστασία προσωπικών δεδομένων
- Πραγματοποίηση ελέγχων συμμόρφωσης των διαδικασιών που εφαρμόζουν τα Εργαστήρια για την προστασία των δεδομένων με τις απαιτήσεις της σχετικής εθνικής και ευρωπαϊκής νομοθεσίας στο σύνολο των δραστηριοτήτων των Εργαστηρίων, αλλά και ανά τμήμα δραστηριότητας
- Σύνταξη, βελτίωση ή/και επικαιροποίηση και υποβολή στη Διοίκηση για έγκριση διαδικασιών, πολιτικών, εντύπων και αρχείων σχετικά με την ασφαλή επεξεργασία και προστασία των δεδομένων
- Υποδείξεις, προτάσεις και συμβουλές για την ανάγκη διεξαγωγής εκτίμησης αντικτύπου για την προστασία των δεδομένων (DPIA) και παρακολούθηση της υλοποίησης/εφαρμογή της

- Εκπόνηση Εκτίμησης Αντικτύπου σχετικά με την προστασία δεδομένων (DPIA), εφόσον χρειάζεται, σε συνεργασία με τον Υπεύθυνο Ασφάλειας Πληροφορικών και αρμόδιων στελεχών των Εργαστηρίων
- Συνεργασία με τον Υπεύθυνο Ασφάλειας Πληροφοριών στην αντιμετώπιση περιστατικού παραβίασης της ασφάλειας πληροφοριών ή/και προστασίας προσωπικών δεδομένων
- Εκπροσώπηση των Εργαστηρίων ενώπιον αρμοδίων αρχών και συνεργασία με αυτές
- Επικοινωνία με εξωτερικούς Φορείς και τρίτα μέρη για θέματα σχετικά με την προστασία των προσωπικών δεδομένων
- Συμμετοχή σε Διοικητικά Συμβούλια που αφορούν την ασφάλεια των πληροφοριών και την προστασία των προσωπικών δεδομένων
- Εκπαίδευση του προσωπικού των Εργαστηρίων σχετικά με την προστασία των προσωπικών δεδομένων, τους τρόπους ορθής και σύννομης επεξεργασίας αυτών και τον τρόπο συμμόρφωσης με τις διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων και της σχετικής εθνικής και ευρωπαϊκής νομοθεσίας
- Μέριμνα για τη συνεχή ευαισθητοποίηση του προσωπικού και δημιουργία κουλτούρας στα Εργαστήρια για τη σημασία της προστασίας των προσωπικών δεδομένων και τη συμμόρφωση με τις απαιτήσεις της σχετικής νομοθεσίας

4.4 Διευθυντές Τμημάτων

Οι Διευθυντές των Τμημάτων των Εργαστηρίων έχουν τις εξής αρμοδιότητες σε σχέση με την ασφάλεια Πληροφοριών και Δεδομένων:

- Συμμετοχή στον εντοπισμό, την εκτίμηση και το σχεδιασμό της διαχείρισης των κινδύνων που σχετίζονται με τις πληροφορίες, τα δεδομένα και τα πληροφοριακά αγαθά (εξοπλισμός και συστήματα) που διαχειρίζεται το τμήμα τους
- Επίβλεψη της τήρησης του συνόλου των Πολιτικών Πληροφορικής Ασφαλείας και των Διαδικασιών για την προστασία των δεδομένων που εφαρμόζουν τα Εργαστήρια από τα στελέχη του τμήματός τους
- Ενεργός συμμετοχή στην ανασκόπηση περιστατικών ασφαλείας, ώστε να διερευνηθούν οι αιτίες τους και να σχεδιαστούν οι απαραίτητες διορθωτικές ενέργειες.
- Εντοπισμός σημαντικών αλλαγών στις δραστηριότητες του τμήματός τους που μπορεί να επηρεάσουν τις πρακτικές για την ασφάλεια της πληροφορίας και την προστασία των δεδομένων στο τμήμα ευθύνης τους και αναφορά τους στον Υπεύθυνο Ασφάλειας Πληροφοριών ή/και στον Υπεύθυνο Προστασίας Δεδομένων
- Συνεργασία με τον Υπεύθυνο Ασφάλειας Πληροφοριών και στον Υπεύθυνο Προστασίας Δεδομένων για θέματα ασφάλειας πληροφοριών και προστασίας δεδομένων

4.5 Εργαζόμενοι

Όλοι οι εργαζόμενοι των Εργαστηρίων έχουν τις εξής αρμοδιότητες σε σχέση με την ασφάλεια Πληροφοριών και Δεδομένων:

- Εφαρμογή του συνόλου των Πολιτικών Πληροφορικής Ασφαλείας και των Διαδικασιών για την προστασία των δεδομένων που εφαρμόζουν τα Εργαστήρια
- Άμεση αναφορά στον Υπεύθυνο Ασφάλειας Πληροφοριών και στον Υπεύθυνο Προστασίας Δεδομένων οποιουδήποτε περιστατικού ασφαλείας ή προστασίας δεδομένων εμπίπτει στην αντίληψή τους

5 Πολιτική Ασφάλειας Πληροφοριών

5.1 Απαιτήσεις Ασφάλειας Πληροφοριών

Οι απαιτήσεις για την ασφάλεια των πληροφοριών και δεδομένων στα **MEGALAB ΔΙΑΓΝΩΣΤΙΚΑ ΕΡΓΑΣΤΗΡΙΑ** ορίζονται σαφώς στις επιμέρους Πολιτικές Ασφαλείας και οι πρακτικές δραστηριότητας των Εργαστηρίων επικεντρώνονται στην εφαρμογή των απαιτήσεων αυτών. Επιπλέον, οι κανονιστικές, ρυθμιστικές και συμβατικές απαιτήσεις τεκμηριώνονται και λαμβάνονται υπόψη στη διαδικασία σχεδιασμού των πολιτικών και διαδικασιών των Εργαστηρίων. Ειδικές απαιτήσεις όσον αφορά την ασφάλεια νέων ή τροποποιημένων συστημάτων, δραστηριοτήτων ή υπηρεσιών θα αποτελούν μέρος του σταδίου σχεδιασμού κάθε έργου.

Είναι θεμελιώδης αρχή των **MEGALAB ΔΙΑΓΝΩΣΤΙΚΩΝ ΕΡΓΑΣΤΗΡΙΩΝ** ότι το σύνολο των Πολιτικών Πληροφορικής Ασφαλείας και των Διαδικασιών για την προστασία των δεδομένων και οι έλεγχοι που το υποστηρίζουν εξυπηρετούν τις επιχειρηματικές ανάγκες των Εργαστηρίων και αυτό θα επικοινωνείται τακτικά σε όλο το ανθρώπινο δυναμικό των Εργαστηρίων μέσω εκπαιδεύσεων, ομαδικών συναντήσεων και γραπτών ενημερώσεων.

5.2 Πλαίσιο για τον καθορισμό στόχων

Ο καθορισμός στόχων σχετικά με την ασφάλεια των πληροφοριών πραγματοποιείται περιοδικά, ώστε να συμπίπτει με τον προγραμματισμό του προϋπολογισμού. Με τον τρόπο αυτό εξασφαλίζεται επαρκής χρηματοδότηση για τις ενέργειες βελτίωσης που εντοπίζονται ή/και προγραμματίζονται. Οι στόχοι αυτοί βασίζονται σε σαφή κατανόηση των επιχειρηματικών απαιτήσεων των Εργαστηρίων.

Οι στόχοι για την ασφάλεια των πληροφοριών έχουν συμφωνημένο χρονοδιάγραμμα και πλάνο υλοποίησής τους. Αυτά αξιολογούνται και παρακολουθούνται ως μέρος των ανασκοπήσεων της διοίκησης ώστε να διασφαλίζεται η εγκυρότητά τους.

Τα **MEGALAB ΔΙΑΓΝΩΣΤΙΚΑ ΕΡΓΑΣΤΗΡΙΑ** πραγματοποιούν τακτικούς και έκτακτους ελέγχους για την ασφάλεια των πληροφοριών και δεδομένων. Τα ευρήματα των ελέγχων επανεξετάζονται σε τακτική βάση σε συνδυασμό με τα αποτελεσμάτα από τις εκτιμήσεις κινδύνου και παράλληλα με τα σχέδια διαχείρισης κινδύνου ασφάλειας πληροφοριών.

Επιπλέον, εφαρμόζονται ενισχυμένοι ή/και συμπληρωματικοί έλεγχοι, όποτε κρίνεται αναγκαίο σύμφωνα με τους γενικά αναγνωρισμένους κώδικες πρακτικής (Codes of Practice), βοηθώντας έτσι ακόμα περισσότερο στη συμμόρφωση των **MEGALAB ΔΙΑΓΝΩΣΤΙΚΩΝ ΕΡΓΑΣΤΗΡΙΩΝ** με τις διεθνείς απαιτήσεις και διατάξεις για την ασφάλεια των πληροφοριών και την προστασία των δεδομένων.

5.3 Συνεχής Βελτίωση της Ασφάλειας Πληροφοριών

Τα **MEGALAB ΔΙΑΓΝΩΣΤΙΚΑ ΕΡΓΑΣΤΗΡΙΑ** μεριμνούν συνεχώς για τη συνεχή βελτίωση της Πολιτικής Ασφάλειας Πληροφοριών και Δεδομένων που εφαρμόζουν με στόχο:

- Τη συνεχή βελτίωση της αποτελεσματικότητας των ελέγχων για την ασφάλεια των πληροφοριών
- Τη συνεχή βελτίωση των εφαρμοζόμενων διαδικασιών και την ευθυγράμμισή τους με τις καλές πρακτικές, όπως αυτές ορίζονται από τα σχετικά πρότυπα
- Την αύξηση των προληπτικών ενεργειών αναφορικά με την ασφάλεια των πληροφοριών
- Να καταστήσουν τις διαδικασίες και τα σημεία ελέγχων της ασφάλειας πληροφοριών περισσότερο μετρήσιμα ώστε να παρέχουν μια γερή βάση για τεκμηριωμένες αποφάσεις
- Τις προτάσεις για βελτίωση μέσω τακτικών συναντήσεων και άλλων μορφών επικοινωνίας με τα ενδιαφερόμενα μέρη
- Την αναθεώρηση των προτάσεων για βελτίωση σε τακτικές συνεδριάσεις της Διοίκησης, προκειμένου να δίνονται προτεραιότητες και να αξιολογούνται τα χρονοδιαγράμματα και τα οφέλη.

Προτάσεις για βελτίωση μπορούν να λαμβάνονται από οποιαδήποτε πηγή, συμπεριλαμβανομένων των εργαζομένων, των πελατών, των προμηθευτών, του προσωπικού του τμήματος πληροφορικής, των εκτιμήσεων κινδύνου και διαφόρων αναφορών. Οι προτάσεις βελτίωσης καταγράφονται και αξιολογούνται ως μέρος των ανασκοπήσεων της Διοίκησης.

5.4 Εφαρμογή της Πολιτικής Ασφάλειας Πληροφοριών και Δεδομένων

Τα **MEGALAB ΔΙΑΓΝΩΣΤΙΚΑ ΕΡΓΑΣΤΗΡΙΑ** έχουν αναπτύξει και εφαρμόζουν ένα σύνολο Πολιτικών Ασφαλείας σε ένα ευρύ φάσμα δραστηριοτήτων που σχετίζονται με την ασφάλεια των πληροφοριών. Οι πολιτικές αυτές υποστηρίζουν την παρούσα Πολιτική Ασφάλειας Πληροφοριών και Δεδομένων και καθορίζουν τον επιμέρους τρόπο εφαρμογής της.

Στον πίνακα που ακολουθεί αναφέρονται οι επιμέρους μεμονωμένες Πολιτικές με συνοπτική παρουσίαση του περιεχομένου τους και ποιους αφορούν.

megalab
ΔΙΑΓΝΩΣΤΙΚΑ ΕΡΓΑΣΤΗΡΙΑ

Τίτλος Πολιτικής	Αφορά	Απευθύνεται
Πολιτική Ορθής Χρήσης	Ορθή και ασφαλής χρήση των πληροφοριακών συστημάτων, εξοπλισμού και υποδομών των Εργαστηρίων	Σύνολο των εργαζομένων
Πολιτική Φορητών Συσκευών	Ασφάλεια και ασφαλής χρήση φορητών συσκευών, όπως φορητοί υπολογιστές, tablets, smartphones, μέσα εξωτερικής αποθήκευσης (Hard Disk Drives, USB sticks κλπ.)	Χρήστες φορητών συσκευών είτε αυτές παραχωρούνται από τα Εργαστήρια είτε είναι προσωπικές αλλά χρησιμοποιούνται και για επαγγελματικούς σκοπούς
Πολιτική Ελέγχου Πρόσβασης	Εγγραφή και διαγραφή χρηστών, παροχή δικαιωμάτων πρόσβασης, εξωτερική πρόσβαση, αναθεωρήσεις πρόσβασης, πολιτική κωδικών πρόσβασης, ευθύνες χρήστη και έλεγχος πρόσβασης συστήματος και εφαρμογών	Εργαζόμενοι που εμπλέκονται στη δημιουργία και διαχείριση του ελέγχου πρόσβασης
Πολιτική Κρυπτογράφησης	Εκτίμηση κινδύνου, επιλογή τεχνικών, ανάπτυξη, δοκιμή και ανασκόπηση της κρυπτογράφησης και διαχείριση των κλειδιών κρυπτογράφησης	Εργαζόμενοι που εμπλέκονται στη δημιουργία και τη διαχείριση της χρήσης τεχνολογίας και τεχνικών κρυπτογράφησης
Πολιτική Φυσικής Ασφάλειας	Ασφαλείς περιοχές, ασφάλεια χαρτιού και εξοπλισμού και διαχείριση κύκλου ζωής εξοπλισμού	Σύνολο των εργαζομένων
Πολιτική κατά των κακόβουλων προγραμμάτων (anti-malware)	Firewalls, anti-virus, φιλτράρισμα ανεπιθύμητων μηνυμάτων, εγκατάσταση και σάρωση λογισμικού, διαχείριση ευπάθειας, εκπαίδευση και ευαισθητοποίηση χρηστών, παρακολούθηση απειλών και ειδοποιήσεις, τεχνικές ανασκοπήσεις και διαχείριση περιστατικών κακόβουλου λογισμικού.	Εργαζόμενοι που είναι υπεύθυνοι για την προστασία της υποδομής του οργανισμού από κακόβουλο λογισμικό

Τίτλος Πολιτικής	Αφορά	Απευθύνεται
Πολιτική Ασφάλειας Δικτύου	Σχεδιασμός ασφάλειας δικτύου, συμπεριλαμβανομένου του διαχωρισμού δικτύου, της περιμετρικής ασφάλειας, των ασύρματων δικτύων και της απομακρυσμένης πρόσβασης. Διαχείριση της ασφάλειας δικτύων, συμπεριλαμβανομένων των ρόλων και των αρμοδιοτήτων, καταγραφή, παρακολούθηση και αλλαγές.	Εργαζόμενοι υπεύθυνοι για το σχεδιασμό, την υλοποίηση και τη διαχείριση δικτύων
Πολιτική Ηλεκτρονικών Μηνυμάτων	Αποστολή και λήψη ηλεκτρονικών μηνυμάτων, παρακολούθηση των υποδομών ηλεκτρονικής ανταλλαγής μηνυμάτων και χρήση ηλεκτρονικού ταχυδρομείου.	Χρήστες των υποδομών ηλεκτρονικής ανταλλαγής μηνυμάτων
Πολιτική Cloud Computing	Δέουσα επιμέλεια, εγγραφή, εγκατάσταση, διαχείριση και αφαίρεση των υπηρεσιών υπολογιστικού νέφους (Cloud Computing).	Εργαζόμενοι που εμπλέκονται στην προμήθεια και διαχείριση υπηρεσιών cloud.
Πολιτική Λήψης Αντιγράφων Ασφαλείας (Back-up)	Σχεδιασμός, εφαρμογή, τήρηση και παρακολούθηση λήψης αντιγράφων ασφαλείας	Εργαζόμενοι υπεύθυνοι για την τήρηση αντιγράφων ασφαλείας
Πολιτική Τηλε-εργασίας	Μέσα και μέθοδοι για την ορθή λειτουργία των Εργαστηρίων σε συνθήκες τηλε-εργασίας	Όλοι οι εργαζόμενοι που εργάζονται απομακρυσμένα (σε τακτική ή έκτακτη βάση)
Πολιτική Λειτουργίας Συστήματος Βιντεοεπιτήρησης (CCTV)	Σχεδιασμός και ορθή λειτουργία συστήματος βιντεοεπιτήρησης στις εγκαταστάσεις των Εργαστηρίων	Σύνολο των εργαζομένων
Πολιτική Προστασίας Δεδομένων	Επεξεργασία δεδομένων προσωπικού χαρακτήρα (Προσωπικά Δεδομένα) σε όλες τις δραστηριότητες των Εργαστηρίων	Εργαζόμενοι που είναι υπεύθυνοι για το σχεδιασμό, τη διαχείριση ή τη χρήση συστημάτων που επεξεργάζονται προσωπικά δεδομένα

megalab
ΔΙΑΓΝΩΣΤΙΚΑ ΕΡΓΑΣΤΗΡΙΑ